

Kaseya 2

Mobile Device Management

Benutzerhandbuch

Versión 7.0

Deutsch

September 15, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Überblick der Endpunkte von mobilen Geräten

Mobile Device Management (KMDM) liefert IT-Unternehmen die Sichtbarkeit, die sie brauchen, um mobile Geräte effizient, konsequent und verlässlich nachzuverfolgen, zu aktualisieren und zu sichern. Mit dem **Mobile Device Management**-Modul können IT-Unternehmen mobile Geräte mit demselben IT Automation Framework von Kaseya verwalten, mit dem auch Desktops, Laptops und Server verwaltet werden.

Auf jedem verwalteten Gerät, das Textnachrichten oder einen Weblink nutzt, wird eine **Kaseya Agent**-Anwendung bereitgestellt, die als Agent auf dem mobilen Gerät wirkt. Nach der Installation hat der Administrator vollständigen Einblick in Hardware und Software des Geräts, einschließlich Seriennummer, Betriebssystem, Firmware-Status, installierte Anwendungen und andere Inventardaten.

Aufgrund der proprietären Art von Mobilfunknetzen und mobilen Geräten muss die **Kaseya Agent**-Anwendung autonomer sein, Bandbreite sparen und sicherstellen, dass Ausführungen dann geschehen, wenn das Gerät nicht in einem Netzwerk angemeldet ist. Ausführungen der **Kaseya Agent**-Anwendung können manuell von einem Administrator ausgelöst werden oder so eingestellt werden, dass sie automatisch beim Erreichen bestimmter Grenzwerte oder Ereignisse geschehen.

Vorteile

- Erweitert Richtlinien für IT-System-Management auf mobile Geräte, einschließlich iPhone, iPad, Android-Telefone, Blackberry und Tablets.
- Schützt Unternehmensdaten an jedem Ort.
- Verringert die Anzahl von Helpdesk-Anfragen, wie z. B. mobile E-Mail-Konfiguration durch automatische und Remote-Verwaltungsfunktionen.
- Verwaltet alle Geräte – von Desktops und Servern bis hin zu mobilen Geräten – von einem Bildschirm aus und sorgt so für Konsistenz und Transparenz innerhalb des Unternehmens.

Merkmale

- Automatisiert E-Mail-Konfiguration und -Einstellungen auf einem oder mehreren Geräten.
- Prüft jedes verwaltete Gerät und liefert eine detaillierte Inventarisierung von verwendeter Hardware, Betriebssystemen und Anwendungen.
- Verfolgt den Standort von mobilen Geräten in Echtzeit nach und speichert den Standortverlauf.
- Löst auf den Geräten einen Alarm aus, sodass Benutzer ihre verlorenen Geräte wiederfinden können.
- Sperrt und löscht verlorene bzw. gestohlene Geräte und setzt sie zurück.
- Sichert Kontaktlisten auf mobilen Geräten und stellt sie wieder her.
- Sendet Textnachrichten von VSA an mobile Geräte.

Funktionen	Beschreibung
Mobiler Workflow *(siehe 9)*	Zeigt Workflows für eine Vielzahl von Modulaktivitäten an.
Dashboard *(siehe 9)*	Bietet eine Übersicht des Status aller vom Modul verwalteter Geräte.
Gerätestatus *(siehe 10)*	Installiert und deinstalliert die Mobile Device Management-Verwaltungsanwendung auf mobilen Geräten.
Geräteübersicht *(siehe 13)*	Plant Audits von Software- und Hardwareattributen eines ausgewählten Geräts und führt sie aus.
Gerät-Nachrichten	Erstellt und sendet Nachrichten, die auf ausgewählten

(siehe 17)	mobilen Geräten als Pop-up-Nachrichten angezeigt werden.
Verlorene Geräte *(siehe 35)*	Markiert Geräte als verloren und startet zusätzliche Aktionen, um verlorene Geräte zu finden und wiederherzustellen.
Kontakte *(siehe 20)*	Sichert Kontaktlisten auf Geräten und stellt sie wieder her.
Anwendungsprotokolle *(siehe 21)*	Zeigt ein Protokoll der Mobile Device Management-Aktivität an.
Mehrere Geräte lokalisieren *(siehe 22)*	Zeigt die aktuellen Standorte von ausgewählten Geräten an.
Ein einziges Gerät nachverfolgen *(siehe 23)*	Zeigt Standortverfolgungsdaten für ein ausgewähltes Gerät an.
Profile erstellen *(siehe 28)*	Definiert Konfigurationsprofile, die Geräten zugewiesen werden können.
Profile zuweisen *(siehe 36)*	Weist Konfigurationsprofile ausgewählten Geräten zu.
Gerätebenachrichtigungen *(siehe 36)*	Konfiguriert Benachrichtigungen für Geräte.
Gruppenbenachrichtigungen *(siehe 37)*	Konfiguriert Benachrichtigungen für alle Geräte in einem Unternehmen oder einer Rechnergruppe.
Systemeinstellungen *(siehe 42)*	Stellt Systemoptionen für das Mobile Device Management-Modul ein.
Server-Einstellungen *(siehe 43)*	Stellt Serveroptionen für das Mobile Device Management-Modul ein.

Mobile Device Management Modulvoraussetzungen

Kaseya Server

- Das Mobile Device Management 7.0-Modul erfordert VSA 7.0.
- Für dieses Modul muss VSA Internetzugang haben.

Anforderungen für jedes verwaltete Gerät

- IOS 6.0 oder höher
- Android 2.3 oder höher
- Blackberry 6.0 oder höher
- Entsperrte Geräte werden nicht unterstützt.

> **Hinweis:** Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Lizenzierung für Mobilgerätverwaltung

Die folgenden Ereignisse wirken sich auf **Mobile Device Management**-Lizenzzahlen aus:

- **Mobile Device Management** Geräte verwenden den gleichen Lizenztyp, der zur Lizenzierung eines auf einem Rechner installierten Agent verwendet wird.

- Eine Lizenz wird als "verwendet" gezählt, wenn das mobile Gerät sein erstes Audit abgeschlossen hat und bestätigt, dass die **Kaseya Agent**-Anwendung installiert ist.
- Wenn das Konto in **Mobile Device Management** gelöscht wird, ungeachtet dessen, was mit der **Kaseya Agent**-Anwendung auf dem Gerät geschieht, erhält die Lizenz wieder den Status "nicht verwendet".

Installieren der Kaseya Agent-Anwendung

Mobile Device Management bietet zwei Möglichkeiten, ein Konto zu erstellen und die **Kaseya Agent**-Anwendung auf einem Gerät zu installieren.

- **Ein Konto erstellen und eine Einladung senden** – *Wird zur Registrierung eines einzelnen Geräts verwendet, das eine Telefonnummer hat.* Sofort nachdem das Konto auf der Seite **Gerätestatus** *(siehe 10)* erstellt wurde, wird eine SMS an die Telefonnummer des Geräts gesendet. Die SMS fordert den Benutzer dazu auf, die **Kaseya Agent**-Anwendung auf diesem Gerät zu installieren und bietet einen Link zum Download. Da die Nachricht von einem bestimmten VSA erstellt und gesendet wurde, muss der Benutzer nicht angeben, bei welchen VSA sich die **Kaseya Agent**-Anwendung anmelden soll. Diese Informationen sind in der SMS für die **Kaseya Agent**-Anwendung enthalten, die bei der Installation der **Kaseya Agent**-Anwendung zu verwenden ist. Nach der Installation meldet sich die **Kaseya Agent**-Anwendung zum ersten Mal in **Mobile Device Management** an und füllt die Registrierung des Geräts aus. Die **Kaseya Agent**-Anwendung kann von einer dieser drei Websites heruntergeladen werden:
  - **Google Play** *(https://market.android.com/details?id=com.kaseya.mdm)*
  - **iTunes App Store** *(http://itunes.apple.com/us/app/kaseya-agent/id458392368?mt=8)*
  - **Blackberry App World** *(http://appworld.blackberry.com/webstore/content/69915/)*
- **Senden Sie eine E-Mail mit der Server-ID** – *Wird verwendet, um mehrere Geräte mit und ohne Telefonnummer zu registrieren.* Der Vorteil dieser Methode besteht darin, dass der VSA-Benutzer nicht jedes Konto vorher manuell erstellen muss. Für jedes **Mobile Device Management**-Modul wird bei seiner ersten Installation auf einem VSA eine eindeutige Server-ID erstellt. Die Server-ID ist auf der Seite **Systemeinstellungen** *(siehe 42)* angegeben. Der VSA-Benutzer muss eine E-Mail mit Anweisungen zum Download der **Kaseya Agent**-Anwendung auf ein Gerät erstellen. Die Anweisungen müssen den Downloadlink und die eindeutige Server-ID enthalten, die der Benutzer nach der Installation der **Kaseya Agent**-Anwendung auf dem Gerät eingibt. Sobald die Server-ID eingegeben ist, meldet sich die **Kaseya Agent**-Anwendung zum ersten Mal an, erstellt das Konto im **Mobile Device Management**-Modul und füllt die Registrierung des Geräts aus. Die E-Mail kann wie folgt aussehen: `Click here to install the Kaseya Agent app: https://mobile.kaseya.com/vsaws/v1 Use this registration code: <yourServerID>"`

Erste Anmeldung:

Bei der ersten Anmeldung der **Kaseya Agent**-Anwendung werden die folgenden Aufgaben auf dem Gerät ausgeführt.

- Ein Audit der Hardwareeinstellungen
- Ein Audit aller auf dem Gerät installierten Anwendungen
- Alle Geräteeinstellungen werden abgerufen
- Der Befehl **Aktuellen Standort abrufen** wird ausgeführt, wenn dies vom Gerät gestattet wird

> **Hinweis:** Siehe **Manuelles Bereitstellen der Mobile Device Management-Anwendung auf Geräten mit Blackberry 5.x** *(http://help.kaseya.com/webhelp/DE/KMDM/7000000/kmdm-blackberry70.pdf#zoom=70&navpanes=0)*

Installationen ohne Agent

Mobile Device Management kann iOS-Geräte verwalten, ohne die Kaseya Agent-Anwendung auf den iOS-Geräten zu installieren. Stattdessen wird ein Zertifikat auf dem Gerät installiert. Das Zertifikat gibt **Mobile Device Management** die Erlaubnis, Befehle an das iOS-Gerät zu senden. Das iOS-Gerät reagiert auf die von **Mobile Device Management** gesendeten Befehle mithilfe der Funktionen des iOS-Betriebssystems und stützt sich nicht auf einen installierten Agent.

Sie können über die Seite **Systemeinstellungen** *(siehe 42)* die Nachrichten anpassen, die als Einladung an iOS-Benutzer gesendet werden, um eine *Installation ohne Agent* vorzunehmen.

Kommunikation mit Geräten

Größtenteils ist die Kommunikation zwischen dem **Mobile Device Management**-Modul und den verwalteten Geräten sowohl für Gerätebenutzer als auch für VSA-Benutzer transparent. Der VSA-Benutzer sollte die folgenden Konzepte kennen, wenn er Befehle an Geräte sendet.

Befehlsverarbeitung

1. Befehle werden für ein Gerät in die Warteschlange gestellt und auf dem Server behalten.
2. Wenn sich die **Kaseya Agent**-Anwendung auf einem Gerät anmeldet, verarbeitet das Gerät jeden Befehl in der Warteschlange.
3. Anmeldungen geschehen in festgelegten Intervallen, es sei denn, ein VSA-Benutzer fordert eine sofortige Anmeldung an.
4. Wenn ein VSA-Benutzer eine sofortige Anmeldung für ein Gerät anfordert, wird eine Nachricht an den Gerätebenutzer gesendet, in der er aufgefordert wird, die **Kaseya Agent**-Anwendung auf dem Gerät zu öffnen, wodurch sich die **Kaseya Agent**-Anwendung sofort anmeldet.

Befehlsstatus

Durch Klicken auf die Schaltfläche **Befehlsstatus** auf der Seite **Gerätestatus** *(siehe 10)* wird der Status jedes Befehls angezeigt, der an ein Gerät gesendet wurde, sowohl beendet als ausstehend. Ein Befehl kann die folgenden Status haben:

- Der Befehl ist ausstehend. Der Agent hat sich noch nicht zum Abrufen angemeldet.
- Der Agent bearbeitet den Befehl.
- Der Vorgang ist abgeschlossen.
- Befehl fehlgeschlagen.

Agent-Anmeldungsintervall

Standardmäßig meldet sich ein Gerät alle 720 Minuten (12 Stunden) bei **Mobile Device Management** an. Bei der Anmeldung werden alle Nachverfolgungsdaten, die seit der letzten Anmeldung gesammelt wurden, an den Server gesendet. Außerdem werden alle Befehle, die auf den Server in Warteschlange stehen, an das Gerät gesendet. Manche Befehle werden mithilfe von Push direkt an Geräte übertragen, die die Push-Funktion unterstützen, wie z. B. iOS-Geräte.

Anfordern einer sofortigen Agent-Anmeldung

Sie können jedes Gerät – iOS und Android – dazu auffordern, sich sofort anzumelden. Durch Klicken auf die Schaltfläche **Check-in anfordern** auf der Seite **Gerätestatus** *(siehe 10)*:

- wird bei iOS eine Nachricht durch AppleMDM gesendet, die auf dem Gerätedisplay angezeigt wird.
- wird bei Android eine Textnachricht an das Gerät gesendet.

In beiden Fällen wird der Gerätebenutzer dazu angewiesen, auf das Symbol der **Kaseya**

Agent-Anwendung zu tippen, um sie zu öffnen. Durch Öffnen der **Kaseya Agent**-Anwendung meldet sich der Anwendungs-Agent sofort an.

Verlängerung der Akkulaufzeit von Geräten

Durch Ausschalten der Gerätenachverfolgung wird die Akkulaufzeit von Geräten am effizientesten verlängert. Auch durch Einstellen des Agent-Anmeldungsintervalls auf ein längeres Intervall wird die Akkulaufzeit von Geräten verlängert.

VSAVSAs ohne Internetverbindung

Mobile Device Management wird in privaten VSA-Netzwerken nicht unterstützt.

Verwalten von verlorenen Geräten

Auf der Seite **Verlorene Geräte** werden Geräte als verloren oder gefunden gekennzeichnet und die Aktionen eingestellt, die durchgeführt werden können. Zu den Aktionen zählen:

- **Gerät als verloren markieren** – Kennzeichnet das Gerät als verloren.
- **Gerät als gefunden markieren** – Kennzeichnet das Gerät als gefunden.
- **Nachricht senden** – Sendet eine Nachricht an das Gerät.
- **Gerät sperren** – Bei Markierung wird das Gerät gesperrt und der Benutzerzugriff verhindert.
- **Alarm auf Gerät auslösen** – Bei Markierung sagt das Gerät bei jedem Einschalten "Dieses Telefon ist gestohlen". Dieser Alarm kann durch Löschen des Geräts deaktiviert werden.
- **Gerät löschen** – Bei Markierung wird das Gerät auf seine Standardeinstellungen zurückgesetzt. Beim Löschen eines Geräts werden alle Benutzerdaten gelöscht, einschließlich der Management-Anwendung/Kaseya Agent-Anwendung. Die Kaseya Agent-Anwendung kann sich nach dem Löschen des Geräts nicht mehr anmelden.
- **Passcode löschen** – Setzt Passcodes auf verwalteten iOS-Geräten zurück. Durch ein Zurücksetzen wird das Gerät entsperrt, wodurch der Benutzer das Gerät entweder ohne Passcode verwenden oder einen neuen Passcode einstellen kann. Durch Löschen des Passcodes wird nicht das darunterliegende Sicherheitsprofil geändert. Wenn das Gerät so konfiguriert ist, dass ein Passcode erforderlich ist, so wird der Benutzer direkt dazu aufgefordert, einen neuen einzugeben.

Sichern und Wiederherstellen von Gerätekontaktliste

Die Seite **Kontakte** sichert Kontaktlisten von Geräten und stellt sie wieder her. Wenn ein Gerät verloren oder gestohlen ist, kann die Kontaktliste auf einem neuen Gerät wiederhergestellt werden. Eventuell muss eine Kontaktliste auch auf einem vorhandenen Gerät wiederhergestellt werden, wenn das Gerät gelöscht (zurückgesetzt) wird und alle Benutzerdaten gelöscht werden. Die Kontaktinformationen, die von einer ausgewählten Sicherung zurückgegeben werden, werden rechts auf der Seite **Kontakte** angezeigt. Wenn mehrere Sicherungen vorhanden sind, können Sie die anzuzeigende Sicherung auswählen.

Nachverfolgung der Standorte von Geräten

Für jedes Gerät, das Standortdaten abgibt, wird ein Standortverlauf gespeichert. **Mobile Device Management**bietet zwei Methoden zum Erfassen von Standortdaten für Geräte.

- **Aktuellen Standort abrufen** – Wenn Sie den Standort eines Geräts nur "bei Bedarf" abrufen müssen, wählen Sie ein Gerät aus und klicken Sie auf die Schaltfläche **Aktuellen Standort abrufen**. Diese Schaltfläche ist auf den Seiten **Gerätestatus** *(siehe 10)*, **Mehrere Geräte lokalisieren** *(siehe 22)* und **Ein einziges Gerät nachverfolgen** *(siehe 23)* verfügbar.
- **Nachverfolgung aktivieren** – Wenn für ein Gerät die Nachverfolgung aktiviert ist, protokolliert das Gerät seine Bewegungen von einem Ort zum anderen. *Standorteinträge werden gefiltert*, je nach den durch das **Geräteort und Tracking-Profil** *(siehe 31)* angegebenen Parametern für das Gerät.

Eine Nachverfolgung in Echtzeit wird nicht unterstützt. Ein gefilterter Satz von Standortdatenpunkten wird in das **Mobile Device Management***-Modul hochgeladen, wenn sich die* **Kaseya Agent***-Anwendung auf dem Gerät anmeldet.* Egal welche Methode zum Erfassen der Standortdaten ausgewählt wird, die Ergebnisse werden auf einer Karte mit den folgenden beiden Seiten angezeigt:

- **Mehrere Geräte lokalisieren** *(siehe 22)*
- **Ein einziges Gerät nachverfolgen** *(siehe 23)*

Verwalten von Geräten mithilfe von Profilen

Die Seite **Profile erstellen** definiert Konfigurationsprofile. Profile legen fest, wie Geräte konfiguriert und mit **Mobile Device Management** verwaltet werden. Jedes Profil stellt eine andere Kombination aus Optionen dar. Änderungen an einem Profil betreffen alle Geräte, die diesem Profil zugewiesen sind. Ein Profil wird Geräten mit Mobile > **Profile zuweisen** *(siehe 36)* zugewiesen.

Profiltypen

- **E-Mail-Profil** *(siehe 29)* – Konfiguriert den E-Mail-Client auf einem verwalteten mobilen Gerät. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.
- **Sicherheitsprofil** *(siehe 30)* – Konfiguriert Richtlinien in Bezug auf die Erstellung von PINs. PINs werden von Gerätebenutzern verwendet, um ihre Geräte zu entsperren.
- **Web Clip-Profil** *(siehe 31)* – Gibt eine Webanwendungsverknüpfung zu einer URL an, auf die das Gerät zugreifen kann. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden
- **iOS 4 Geräte-Funktionsprofil** *(siehe 31)* – Gilt für iOS-Geräte mit einer Version unter iOS 5. Aktiviert und deaktiviert beliebte Funktionen auf Geräten mit iOS 4.
- **iOS-Geräte-Funktionsprofil** *(siehe 32)* – Gilt nur für iOS5, iOS6, iOS7. Aktiviert und deaktiviert beliebte Funktionen auf iOS-Geräten.
- **Geräteort und Tracking-Profil** *(siehe 34)* – Stellt Anmeldungs- und Standortoptionen auf Geräten ein. Dies ist das einzige Profil, das für Blackberrys gilt.
- **Benutzerdefiniertes iOS-Konfigurationsprofil** *(siehe 33)* – Ein Profil, das mithilfe des **iPhone-Konfigurationsprogramms** *(http://support.apple.com/kb/DL1466)* erstellt und in **Mobile Device Management** importiert wurde.
- **WiFi-Profil** *(siehe 35)* – Stellt die WiFi-Optionen auf Geräten ein. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.

Deinstallieren der Kaseya Agent-Anwendung

Wenn das Gerätekonto in VSA gelöscht wird, müssen Sie die Kaseya Agent-Anwendung auf dem Gerät manuell löschen.

Manuelles Löschen der Kaseya Agent-Anwendung vom Gerät

Android

1. Gehen Sie auf dem Gerät zu **Einstellungen > Standort & Sicherheit**.
2. Suchen Sie **Geräteadministratoren wählen** und tippen Sie darauf.
3. Entfernen Sie die Markierung von **Kaseya Agent**.
4. Tippen Sie bei Aufforderung auf **Deaktivieren**. Tippen Sie auf **OK**, um die Deaktivierung zu bestätigen.
5. Gehen Sie zu **Einstellungen > Anwendungen > Anwendungen verwalten** und tippen Sie auf **Kaseya Agent**.
6. Tippen Sie bei Aufforderung auf **Deinstallieren**, um die Anwendung zu entfernen. Tippen Sie auf **OK**, um die Deinstallation zu bestätigen.

iOS

Gilt für iPad, iPod, iTouch und iPhone

1. Suchen Sie das Symbol der **Kaseya Agent**-Anwendung auf dem Gerät.
2. Tippen Sie auf das Symbol und halten Sie es gedrückt. Nach einigen Augenblicken beginnt das Symbol zu "wackeln" und neben jeder App erscheint ein **X**.
3. Tippen Sie auf das **X** neben dem Symbol.
4. Wählen Sie bei Aufforderung **Löschen**, um die Anwendung zu entfernen.

Verwalten von Anwendungen auf Geräten

Mobile Device Management kann Anwendungen auf mobilen Geräten benötigen oder nicht zulassen. Anwendungsprofile bestimmen, welche Anwendungen auf mobilen Geräten installiert werden müssen bzw. nicht installiert werden dürfen. Jedes App-Profil stellt eine andere Kombination aus Anwendungen dar. Alle Anwendungen, die zum selben App-Profil gehören, sind entweder alle erforderlich oder alle nicht zugelassen. Sie können einem einzigen mobilen Geräte mehrere App-Profile zuweisen. Änderungen an einem App-Profil betreffen alle Geräte, die diesem App-Profil zugewiesen sind. Unterstützt die Verwaltung sowohl von Anwendungen, die aus App-Stores heruntergeladen wurden, als auch von proprietären *Unternehmensanwendungen*.

- Die Seite **Anwendungsprofile** *(siehe 24)* zeigt die Anwendungen an, die zu jedem App-Profil gehören, und ob sie erforderlich oder nicht zugelassen sind.
- Verwalteten mobilen Geräten wird ein App-Profil über die Seite **App-Profile zuweisen** *(siehe 26)* zugewiesen.
- Die Seite **App-Katalog** *(siehe 26)* enthält einen Katalog der *App-Elemente*. Ein App-Element ist ein Datensatz, der eine einzelne Anwendung eindeutig identifiziert, welche auf einem mobilen Gerät erforderlich bzw. nicht zugelassen ist.
- Die Seite **App-Bestand** *(siehe 28)* erzeugt eine Liste von App-Elementen basierend auf einem Audit aller von **Mobile Device Management** verwalteten mobilen Geräten. Anstatt Anwendungspositionen manuell im **App-Katalog** anzugeben, können Sie diese Seite verwenden, um ein automatisch erstelltes App-Element zum **App-Katalog** hinzuzufügen.
- Die Registerkarte **App-Konformität** wird aus der Seite **Geräteübersicht** angezeigt. Die Registerkarte zeigt alle erforderlichen Anwendungen an, die auf dem Gerät fehlen, und alle nicht zugelassenen Anwendungen, die auf dem Gerät installiert sind. Die Registerkarte **Anwendung** zeigt alle Anwendungen auf dem Gerät an, ungeachtet ihres Konformitätsstatus.
- Sie werden durch zwei Benachrichtigungsregisterkarten auf der Seite **Gerätebenachrichtigungen** *(siehe 37)* über die App-Konformität informiert: **Nicht zugelassene Apps** und **Erforderliche Apps**

- Sie können über die Seite **Systemeinstellungen** *(siehe 42)* die Nachrichten anpassen, die an Benutzer als Einladung zur Installation einer erforderlichen Anwendung gesendet werden.
- Anw.-Management wird durch zwei Optionen auf der Seite **Servereinstellungen** *(siehe 43)* unterstützt: **Aufbewahrungszeit für Protokolle von App-Einladungen** und **Schwellwert für die Neuversendung von App-Einladungen**.

Moduleinstellungen

Zwei Seiten definieren die Einstellungen für das ganze **Mobile Device Management**-Modul.

- **Systemeinstellungen** *(siehe 42)* – Bietet Standardeinstellungen für Profile, die mit der Seite **Profile erstellen** *(siehe 28)* erstellt wurden.
- **Servereinstellungen** *(siehe 43)* – Konfiguriert die Einstellungen, die für den **Mobile Device Management**-Server oder das gesamte **Mobile Device Management**-Modul gelten.

Benachrichtigungen

Mobile Device Management bietet drei allgemeine Benachrichtigungstypen.

- **Gerätebenachrichtigungen** – Zu den gerätespezifischen Benachrichtigungen zählt:
  - **Gerät offline** – Das Gerät hat sich während der angegebenen Anzahl an Minuten nicht angemeldet.
  - **Verlorenes Gerät checkt ein** – Ein Gerät meldet sich an, nachdem es als verloren gemeldet wurde.
  - **Gerät checkt ein** – Ein Gerät meldet sich an.
  - **Agent auffordern** – Fordert den Benutzer des Geräts auf, nachdem sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet hat. Gilt nur für iOS.
- **Gruppenbenachrichtigungen** – Erstellt eine Benachrichtigung, wenn ein neues Gerät einem angegebenen Unternehmen oder einer Rechnergruppe beitritt.
- **System-Benachrichtigungen** – Erstellt eine Benachrichtigung, wenn eine bestimmte Anzahl von nicht verwendeten Gerätelizenzen verfügbar ist.

Wenn eine **Mobile Device Management**-Benachrichtigung aktiviert ist und die Alarmbedingung eintritt, kann eine E-Mail gesendet oder ein Ticket erstellt werden.

> **Hinweis:** Bei auf mobilen Geräten basierenden Benachrichtigungen werden Benachrichtigungen und das Ausführen von Agent-Verfahren nicht unterstützt.

Protokolle

Es werden zwei Protokolle gepflegt von **Mobile Device Management**

- **Anwendungsprotokoll** – Die Seite **Anwendungsprotokolle** *(siehe 21)* zeigt einen Protokolleintrag von jeder im **Mobile Device Management**-Modul ausgeführten VSA-Benutzeraktion an. Systemereignisse, die vom **Mobile Device Management**-Modul selbst ausgelöst werden, sind nicht enthalten.
- **Geräteprotokoll** – *Das Geräteprotokoll dient nur für Kaseya Support-Zwecke.* Das Geräteprotokoll zeigt die tatsächlichen Nachrichten an, die zwischen VSA und einem ausgewählten Gerät hin- und her gesendet wurden. Da Dienstanbieter diese Informationen nicht benötigen, werden Geräteprotokolle für ein ausgewähltes Gerät nur angezeigt, wenn die Schaltfläche **Protokoll anfordern** auf der Seite **Geräteübersicht** *(siehe 13)* angeklickt wird. Einträge von Geräteprotokollen

werden dann in der Registerkarte **Protokolle** angezeigt. Durch Klicken auf die Schaltfläche **Protokolldetails anzeigen** bei einem bestimmten Protokolleintrag wird der Text der Nachricht angezeigt.

> **Hinweis:** Auf mobilen Geräten basierende Ereignisse und Protokolle werden sonst an keiner Stelle in VSA angezeigt.

Berichte

Die folgenden Berichte werden mit **Mobile Device Management** bereitgestellt. Jeder Bericht kann anhand mehrerer Spalten mit Informationen sortiert und gefiltert werden.

- **Geräteanwendungen** – Zeigt die auf jedem Gerät installierten Anwendungen an.
- **Gerätestatus** – Führt den Status jedes Geräts auf.
- **Geräteübersicht** – Führt Audit-Informationen für jedes Gerät auf.
- **Verlorene Geräte** – Führt alle verlorenen Geräte und die darauf ausgeführten Aktionen auf.

Mobiler Workflow

Mobile > Vorgänge > Mobiler Workflow

Die Seite **Mobiler Workflow** bietet eine Übersicht der Workflows zum Konfigurieren und Betreiben von mobilen Geräten mit **Mobile Device Management**. Für jedes Element im Flussdiagramm stehen Hilfe-Links mit weiteren Informationen bereit.

- **Individuelle Implementierung** – Erstellt ein alleinstehendes **Mobile Device Management**-Konto für ein Gerät und beginnt die Installation der **Kaseya Agent**-Anwendung auf dem Gerät. Die **Kaseya Agent**-Anwendung kann von einer dieser drei Websites heruntergeladen werden:
  - **Google Play** *(https://market.android.com/details?id=com.kaseya.mdm)*
  - **iTunes App Store** *(http://itunes.apple.com/us/app/kaseya-agent/id458392368?mt=8)*
  - **Blackberry App World** *(http://appworld.blackberry.com/webstore/content/69915/)*
- **Massenimplementierung** – Versendet eine E-Mail mit der eindeutigen Server-ID. Benutzer können die E-Mail zur Installation der **Kaseya Agent**-Anwendung auf ihren Geräten verwenden. Wenn sich der Agent zum ersten Mal anmeldet, wird das **Mobile Device Management**-Konto erstellt. Eine Beschreibung zu Massenimplementierungen finden Sie unter **Installieren der Kaseya Agent-Anwendung** *(siehe 3)*.
- **E-Mail-Konfiguration** – Gilt nur für iOS, Version 1.1. Konfigurieren und installieren Sie eine separate E-Mail-Client-Anwendung auf dem verwalteten Gerät.
- **Audit** – Führt ein Audit der Software- und Hardwareattribute des verwalteten Geräts durch.
- **Nachverfolgung** – Verfolgt den Standort des Geräts nach.
- **Verloren und Gefunden** – Kennzeichnet ein Gerät als verloren oder gefunden. Ein verlorenes Gerät kann gesperrt werden, eine Nachricht senden, einen Alarm auslösen oder gelöscht werden. Auf einem iOS-Gerät kann der Passcode gelöscht werden.
- **Backup** – Sichert die Kontaktliste eines Geräts und stellt sie wieder her.

Dashboard

Mobile > Vorgänge > Dashboard

Die Seite **Dashboard** bietet eine Übersicht des Status und der Eigenschaften aller mit **Mobile Device**

Management verwalteten Geräte. Durch Verwendung des Filters "Geräte-ID/Gruppen-ID" oben auf der Seite ändern sich die angezeigten Statistiken. Tortendiagramme zeigen den Prozentsatz und die Gerät-Zähler für jeden aufgeführten Status bzw. jede Eigenschaft im Diagramm an. Fahren Sie mit dem Mauszeiger über ein beliebiges Stück des Tortendiagramms, um einen einzelnen Prozentsatz und Gerät-Zähler hervorzuheben.

- **Gerätestatus** – `Normal`, `Command Pending`, `Invited`
- **Gerätehersteller** – Der Hersteller des Geräts.
- **Aktueller Netzbetreiber des Geräts** – Der Netzbetreiber, den das Gerät derzeit verwendet.
- **Geräte-BS** – Das Betriebssystem, das das Gerät nutzt.
- **Original-Netzbetreiber des Geräts** – Der Original-Netzbetreiber, den das Gerät verwendet.
- **Verlorene Geräte** – `Not lost`, `Lost`, `Wiped`

Gerätestatus

Mobile > Vorgänge > Gerätestatus

Die Seite **Gerätestatus** erstellt und löscht **Mobile Device Management**-Konten für mobile Geräte. Außerdem startet sie die Installation und Deinstallation der Kaseya Agent-Anwendung auf mobilen Geräten. Durch das Importieren von Daten können mehrere **Mobile Device Management**-Konten erstellt werden. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Neu** – Erstellt ein **Mobile Device Management**-Konto für ein mobiles Gerät. Eine Nachricht wird an das Gerät gesendet, die den Benutzer dazu auffordert, die Kaseya Agent-Anwendung auf diesem Gerät zu installieren. Nach der Installation meldet sich die Management-Anwendung in **Mobile Device Management** an und schließt die Registrierung ab.
  - **Landes-Code** – Geben Sie den Landescode ein.
  - **Telefonnummer** – Geben Sie die Telefonnummer ein.
  - **Name** – Geben Sie einen Gerätenamen ein. Dieser Name identifiziert das mobile Gerät in VSA. Dies entspricht der Erstellung eines Rechner-ID-Kontonamens für einen Computer in VSA.
  - **Besitzer** – Der Eigentümer des mobilen Geräts.
  - **E-Mail-Adresse** – Eine E-Mail-Adresse, die diesem Gerät zugeordnet ist; nur für Referenzzwecke.
  - **E-Mail-Konto** – Der Benutzername des E-Mail-Kontos, der einer E-Mail-Adresse zugewiesen ist.
  - **Gruppe** – Die VSA-Rechnergruppe, von der das Gerät Mitglied ist.

    Hinweis: Eine Beschreibung zu *Massenimplementierungen* finden Sie unter **Installieren der Kaseya Agent-Anwendung** *(siehe 3)*.

  - **Registrierungstyp**
    - ✓ **iOS ohne Agent** – Siehe **Installationen ohne Agent** *(siehe 4)*.
    - ✓ **iOS, Android oder Blackberry Agent** – Siehe **Installieren der Kaseya Agent-Anwendung** *(siehe 3)*.
  - **Einladung über**
    - ✓ `SMS` - Wird in der Regel bei Mobiltelefonen verwendet.
    - ✓ `Email` - Wird in der Regel bei Tablets verwendet.
    - ✓ `Email including Android App` - Nur bei Android-Geräten: Umfasst die Kaseya

Agent-Anwendung als Anhang in der E-Mail-Einladung, anstatt die Anwendung von einer URL herunterzuladen.

> **Hinweis:** Das Feld **Geräteeinladungsnachricht** auf der Seite **Systemeinstellungen** *(siehe 42)* zeigt den Text der Einladung an.

- **Einladung erneut senden** – Sendet die Nachricht erneut, die den Benutzer dazu einlädt, die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
- **Bearbeiten** – Ändert die Kontoinformationen, die einem mobilen Gerät zugewiesen sind. Siehe **Neu** oben.
- **Löschen** – Löscht ausgewählte Konten.
- **Importieren** – Erstellt **Mobile Device Management**-Konten für Geräte durch Importieren von formatierten Daten aus einem Bearbeitungstextfeld. Jede Zeile des importierten Texts muss im folgenden Format sein: `first,last,phone number`
- **Befehlsstatus** – Zeigt den Status der Befehle an, die an ein Gerät gesendet wurden.
  - Der Befehl ist ausstehend. Der Agent hat sich noch nicht zum Abrufen angemeldet.
  - Der Agent bearbeitet den Befehl.
  - Der Vorgang ist abgeschlossen.
  - Befehl fehlgeschlagen.
- **Aktuellen Standort abrufen** – Gibt den aktuellen Standort des Geräts auf Anfrage aus, aber verfolgt ihn nicht kontinuierlich nach. Der letzte Standort eines Geräts – abgerufen entweder durch den Befehl **Aktuellen Standort abrufen** oder durch Starten der Nachverfolgung – wird auf einer Karte durch **Mehrere Geräte lokalisieren** *(siehe 22)* angezeigt.
- **Nachverfolgung starten** – Startet die Standortnachverfolgung des Geräts. Nach dem Start können Sie das Gerät auf einer Karte mithilfe von **Ein einziges Gerät nachverfolgen** *(siehe 23)* nachverfolgen.
- **Nachverfolgung anhalten** – Hält die Standortnachverfolgung des Geräts an.
- **Standortverlauf** – Zeigt den Standortverlauf eines Geräts an. Standortdaten werden sowohl durch die Befehle **Aktuellen Standort abrufen** als auch durch Nachverfolgung des Geräts ausgegeben.
- **Check-in anfordern** – Der Gerätebenutzer wird angewiesen, auf das Symbol der **Kaseya Agent**-Anwendung zu tippen, um sie zu öffnen. Durch Öffnen der **Kaseya Agent**-Anwendung meldet sich der Anwendungs-Agent sofort an.
  - Bei iOS wird eine Nachricht durch AppleMDM gesendet, die auf dem Gerätedisplay angezeigt wird.
  - Bei Android wird eine SMS an das Gerät gesendet.
- **Aktualisieren** – Aktualisiert die Seite.

Tabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet

- Keine Antwort
- Wird verarbeitet
- Befehl gesendet – erneut versuchen
- Abmelden
- Befehl gesendet – fehlgeschlagen

- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.

  (leer) - Nachverfolgung ist nicht aktiviert.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Besitzer** – Der Eigentümer des Geräts. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Betriebssystemversion** – Die Version des Betriebssystems, die das Gerät nutzt.
- **Letzter Check-in** – Datum/Uhrzeit, zu der sich die Kaseya Agent-Anwendung auf dem Gerät zum letzten Mal in **Mobile Device Management** angemeldet hat.
- **KMDM-Version** – Die Version der Kaseya Agent-Anwendung auf dem Gerät.
- **Zeitzone** – Die Zeitzone, die das Gerät verwendet.
- **Letzte geografische Breite** – Die letzte geografische Breite, die das Gerät ausgegeben hat.
- **Letzte geografische Länge** – Die letzte geografische Länge, die das Gerät ausgegeben hat.
- **Letztes Audit** – Datum/Uhrzeit des letzten Audits.
- **Nächstes Audit** – Datum/Uhrzeit, an dem das nächste Audit geplant ist.
- **Erster Check-in** – Datum/Uhrzeit, zu der sich die Management-Anwendung zum ersten Mal in **Mobile Device Management** angemeldet hat.
- **E-Mail-Adresse** – Die E-Mail-Adresse, die dem Gerät zugeordnet ist; nur für Referenzzwecke. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **E-Mail-Kontoname** –
- **Build** – Die Build-Nummer des Betriebssystems, das das Gerät nutzt.
- **Hersteller** – Der Hersteller der Gerätehardware.
- **Modellname** – Der Modellname der Gerätehardware.
- **Modell** – Die Modellnummer der Gerätehardware.
- **Funkversion** – Die Version der Modem-Firmware, die das Gerät nutzt. Wird auch als "Basisband" bezeichnet.
- **Intern gesamt** – Der gesamte verfügbare Speicherplatz auf der Hardware.
- **Extern gesamt** – Der gesamte verfügbare externe Speicherplatz .
- **Intern frei** – Auf der Hardware verfügbarer und freier Speicherplatz.
- **Extern frei** – Extern verfügbarer und freier Speicherplatz.
- **Seriell** – Die Seriennummer des Geräts.
- **IMEI** – Der eindeutige Bezeichner der Haupt-Assembly des Geräts, unabhängig von der im Gerät eingelegten SIM-Karte. Die IMEI-Nummer gilt für GSM-, WCDMA- und iDEN-Mobiltelefone.

- **ICC** – Der eindeutige Bezeichner der im Gerät eingelegten SIM-Karte.
- **Datenroaming** – `True` oder `False`.
- **WiFi MAC** – Die MAC-ID des Geräts.
- **Original-Netzbetreiber** – Der Hauptdienstanbieter des Geräts.
- **Home-MCC** – Der originale Mobile Country Code des Geräts. Große Länder können mehr als einen Mobile Country Code haben.
- **Home-MNC** – Der Mobile Network Code für den Originalbetreiber/Carrier des Geräts.
- **Aktueller Carrier** – Der Netzbetreiber, den das Gerät derzeit verwendet.
- **Aktueller MCC** – Der Mobile Country Code, den das Gerät derzeit verwendet.
- **Aktueller MNC** – Der Mobile Network Code des Betreibers/Carrier, den das Gerät derzeit verwendet.

Geräteübersicht

Mobile > Vorgänge > Geräteübersicht

Die Seite **Geräteübersicht** plant Audits von Software- und Hardwareattributen eines ausgewählten Geräts und führt sie aus. Alle Audit-Informationen, die für ein einzelnes, ausgewähltes Gerät erfasst werden, werden auf mehreren Registerkarten im unteren Bereich der Seite angezeigt. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Ein Audit planen** – Plant ein Audit für eine bestimmte Zeit auf einem ausgewählten Gerät. Planen Sie eine einmalige oder periodische Ausführung. Bei jeder Art der Wiederholung (einmal, stündlich, täglich, wöchentlich, monatlich) werden weitere verfügbare Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Mögliche Optionen:
  - **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Wenn die geplante Uhrzeit für eine Aufgabe z. B. 03:00 Uhr ist und das Verteilungsfenster eine Stunde anzeigt, dann wird die Aufgabenplanung so geändert, dass sie zu einem beliebigen Zeitpunkt zwischen 03:00 und 04:00 Uhr ausgeführt wird.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Folgenden Zeitrahmen ausschließen – Gilt nur für das Verteilungsfenster.** Bei Markierung ist ein Zeitrahmen angegeben, in dem die Planung einer Aufgabe im Verteilungsfenster ausgeschlossen wird. Die Angabe eines Zeitrahmens außerhalb des Verteilungsfensters wird vom Planer ignoriert.
- **Audit jetzt ausführen** – Führt ein Audit eines ausgewählten Geräts aus.
- **Protokolle anfordern** – *Das Geräteprotokoll dient nur für Kaseya Support-Zwecke.* Das Geräteprotokoll zeigt die tatsächlichen Nachrichten an, die zwischen VSA und einem ausgewählten Gerät hin- und her gesendet wurden. Da Dienstanbieter diese Informationen nicht

benötigen, werden Geräteprotokolle für ein ausgewähltes Gerät nur angezeigt, wenn die Schaltfläche **Protokoll anfordern** auf der Seite **Geräteübersicht** angeklickt wird. Einträge von Geräteprotokollen werden dann in der Registerkarte **Protokolle** angezeigt. Durch Klicken auf die Schaltfläche **Protokolldetails anzeigen** bei einem bestimmten Protokolleintrag wird der Text der Nachricht angezeigt.

- **Aktualisieren** – Aktualisiert die Seite.

Tabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.

  (leer) - Nachverfolgung ist nicht aktiviert.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Letzter Check-in** – Datum/Uhrzeit, zu der sich die Kaseya Agent-Anwendung auf dem Gerät zum letzten Mal in **Mobile Device Management** angemeldet hat.
- **Letztes Audit** – Datum/Uhrzeit des letzten Audits.
- **Nächstes Audit** – Datum/Uhrzeit, zu der das nächste Audit geplant ist.
- **Erster Check-in** – Datum/Uhrzeit, zu der sich die Management-Anwendung zum ersten Mal in **Mobile Device Management** angemeldet hat.
- **E-Mail-Adresse** – Die E-Mail-Adresse, die dem Gerät zugeordnet ist; nur für Referenzzwecke. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.

Alle anderen Felddefinitionen finden Sie im Abschnitt "Registerkarte "Allgemein"" unten.

Registerkarte "Allgemein"

Betriebssystem

- **Typ** – Der Typ des Betriebssystems auf dem Gerät.
- **Betriebssystemversion** – Die Version des Betriebssystems, die das Gerät nutzt.
- **Build** – Die Build-Nummer des Betriebssystems.

Gerätedaten

- **Name** – Der Name, den das Gerät zur eigenen Identifikation verwendet. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Agent-ID** – Die Kaseya Agent-GUID.
- **Gerätebezeichner** – Ein eindeutiger Bezeichner, der dem Gerät vom Hersteller zugewiesen wurde. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Seriell** – Die Seriennummer des Geräts.
- **IMEI** – Der eindeutige Bezeichner der Haupt-Assembly des Geräts, unabhängig von der im Gerät eingelegten SIM-Karte. Die IMEI-Nummer gilt für GSM-, WCDMA- und iDEN-Mobiltelefone.
- **ICC** – Der eindeutige Bezeichner der in ein Gerät eingelegten SIM-Karte.
- **KMDM-Version** – Die Version der **Kaseya Agent**-Anwendung auf dem Gerät.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer. Klicken Sie **Bearbeiten** auf der Seite **Gerätestatus** *(siehe 10)*, um diesen Wert zu ändern.
- **Datenroaming** – `True` oder `False`.
- **WiFi MAC** – Die MAC ID des Geräts.

Ort

- **Zeitzone** – Die Zeitzone, die das Gerät verwendet.
- **Letzte geografische Breite** – Die letzte geografische Breite, die das Gerät ausgegeben hat.
- **Letzte geografische Länge** – Die letzte geografische Länge, die das Gerät ausgegeben hat.

Plattform

- **Hersteller** – Der Hersteller der Gerätehardware.
- **Modellname** – Der Modellname der Gerätehardware.
- **Modell** – Die Modellnummer der Gerätehardware.
- **Funkversion** – Die Version der Modem-Firmware, die das Gerät nutzt. Wird auch als "Basisband" bezeichnet.
- **Intern gesamt** – Der gesamte verfügbare Speicherplatz auf der Hardware.
- **Extern gesamt** – Der gesamte verfügbare externe Speicherplatz .
- **Intern frei** – Auf der Hardware verfügbarer und freier Speicherplatz.
- **Extern frei** – Extern verfügbarer und freier Speicherplatz.

Heimat-Netzwerk

- **Original-Netzbetreiber** – Der Hauptdienstanbieter des Geräts.
- **Home-MCC** – Der originale Mobile Country Code des Geräts. Große Länder können mehr als einen Mobile Country Code haben.
- **Home-MNC** – Der Mobile Network Code für den Originalbetreiber/Carrier des Geräts.

Aktuelles Netzwerk

- **Aktueller Carrier** – Der Netzbetreiber, den das Gerät derzeit verwendet.
- **Aktueller MCC** – Der Mobile Country Code, den das Gerät derzeit verwendet.
- **Aktueller MNC** – Der Mobile Network Code des Betreibers/Carrier, den das Gerät derzeit verwendet.

Registerkarte "Einstellungen"

Diese Geräteeinstellungen werden durch Zuweisen eines **Geräteorts und Tracking-Profils** *(siehe 34)* zu einem Gerät vorgenommen.

- **Check-in nur bei Verbindung mit WiFi** – Bei Markierung meldet sich die Kaseya Agent-Anwendung nur an, wenn eine WiFi-Verbindung verfügbar ist. Ist diese Option nicht markiert, meldet sich die Kaseya-Anwendung per Mobilfunknetz an, wenn keine WiFi-Verbindung verfügbar ist.
- **Gerät nachverfolgen** – Bei Markierung ist Nachverfolgen aktiviert. Standortdaten werden anhand einiger vordefinierter Parameter gefiltert, um sicherzustellen, dass nur genaue und nützliche Standortdaten tatsächlich an VSA gesendet werden. *Aufgezeichnete Standortdaten werden erst an VSA gesendet, wenn der Agent sich zum nächsten Mal anmeldet.* Es werden folgende allgemeine Kriterien verwendet:
  - **Genauigkeit** – Jede Standortaktualisierung von einem GPS-Turm oder -Satelliten verfügt über eine Genauigkeitsbewertung, die einschätzt, wie sehr der Genauigkeit der Standortdaten aus der GPS-Quelle vertraut werden kann.
  - **Alter** – Ein Gerät speichert Standortdaten zwischen und überträgt manchmal alte Standortdaten an die **Kaseya Agent**-Anwendung, wenn seit längerer Zeit keine neue Standortaktualisierung abgerufen wurde.
  - **Zurückgelegte Distanz** – Die Strecke, die das Gerät seit der letzten Standortaktualisierung zurückgelegt hat. Diese kann null sein, wenn sich das Gerät nicht bewegt hat.
- **Anmeldezeit des Agent (Minuten)** –*Dieses Feld wird von installierten Agents ignoriert, die Version 1.1 oder höher der Kaseya Agent-Anwendung verwenden.* Stellt die Mindestdauer zwischen Anmeldeversuchen ein. Eine Anzahl von Umwelt- und Gerätebetriebsfaktoren bestimmt genau, wann die Anmeldung stattfindet. Je kleiner dieser Wert ist, umso mehr Akkustrom wird verbraucht.
- **Verfolgungspräzision (Meter)** – Dieser Wert wird an den GPS-Empfänger gesendet als Hinweis, wie genau die Durchgabe der Standortinformationen sein sollte. Je genauer die Anfrage ist, d. h. je kleiner der Wert, umso länger dauert der Standortabruf und umso mehr Strom wird verbraucht.
- **Mindestgenauigkeit vor Ignorieren (Meter)** – Dieser Wert regelt, welche Standortinformationen als nützlich genug angesehen werden, um an VSA gesendet und gespeichert zu werden. Wenn sich ein Gerät schnell bewegt – z. B. in einem Auto oder einem Zug – sind die Informationen der Standortnachverfolgung weniger genau und irgendwann nicht mehr nützlich. Standortpunkte, die weniger genau als dieser Wert sind, werden herausgefiltert und weder aufgezeichnet noch an VSA gesendet. Dieser Wert bestimmt mehr als alle anderen die Menge und Qualität der Standortinformationen, die vom Gerät gesendet werden.
- **Distanz für Verfolgungsbewegung** – Dieser Wert definiert die Mindestdistanz, die ein Gerät zurücklegen muss, in Metern, damit ein Standortaktualisierungsereignis ausgelöst und an den Agent gesendet wird. Es wird auch vom Agent verwendet, um zu entscheiden, ob der Standortpunkt aufgezeichnet und an VSA gesendet werden soll. Wenn dieser Wert zum Beispiel auf 500 Meter eingestellt ist und sich das Gerät nur 10 Meter bewegt, zeichnet der Agent diesen Punkt nur auf, wenn die **Min. / Max. Verfolgungszeit (Minuten)** dies zulässt.
- **Min. / Max. Verfolgungszeit (Minuten)** – Diese Werte definieren, wie oft Standortinformationspunkte aufgezeichnet werden sollen. Der Mindestwert definiert die Mindestzeit zwischen Punkten. Wenn der Wert zum Beispiel 10 Minuten beträgt, dann werden die an den Agent gemeldeten Standortinformationen nach Meldung eines gültigen Standorts mindestens 10 Minuten lang nicht aufgezeichnet bzw. an VSA gesendet. Wenn jedoch innerhalb der vom maximalen Wert festgelegten Dauert kein gültiger Standortpunkt aufgezeichnet wurde, dann *wird* dieser Punkt aufgezeichnet, ohne Rücksicht auf Genauigkeit oder zurückgelegte Strecke.

Ein Beispiel für die Aufzeichnung eines Punkts:

- Ein Punkt wird bei angemessener Verfolgungsgenauigkeit abgefragt.
- Wenn der zurückgegebene Punkt einen höheren Genauigkeitswert als unter "Mindestgenauigkeit vor Ignorieren" angegeben hat, dann wird er verworfen.
- Wenn das Gerät nicht mindestens die unter "Distanz für Verfolgungsbewegung" angegebene Strecke zurückgelegt hat, wird der Punkt verworfen.

- Wenn die verstrichene Zeit zwischen diesem Punkt und dem letzten aufgezeichneten kürzer als die "Min. Verfolgungszeit" ist, wird der Punkt verworfen.
- Wenn die verstrichene Zeit zwischen diesem Punkt und dem letzten aufgezeichneten länger als die "Max. Verfolgungszeit" ist, dann wird der Punkt aufgezeichnet, auch wenn er durch die vorangehenden Prüfungen verworfen worden wäre.

Registerkarte "Anwendungen"

Die Registerkarte **Anwendungen** zeigt eine Liste der Anwendungen an, die auf dem ausgewählten verwalteten mobilen Gerät installiert sind.

Registerkarte "App-Konformität"

Die Registerkarte **App-Konformität** zeigt zwei App-Konformitätslisten für ein ausgewähltes mobiles Gerät an. Weitere Informationen finden Sie unter **Verwalten von Anwendungen auf Geräten** *(siehe 7)*.

- **Erforderliche Apps, die auf Gerät fehlen**
- **Nicht zugelassene Apps auf Gerät**

Tabellenspalten

- **(App-Typ)**
  - **Store-App** – Bei Auswahl muss eine URL **angegeben werden.**
  - **Unternehmens-App** – Bei Auswahl muss eine **App-Programmdatei** angegeben werden.
- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.
- **Version** – Die Versionsnummer der Anwendung. Beispiel: `1.2.0.0`.
- **Zuletzt gesendete Einladung** – Datum/Uhrzeit, zu der eine Einladung zur Installation dieser Anwendung zuletzt an das mobile Gerät gesendet wurde.

Registerkarte "Protokolle"

Die Registerkarte **Protokolle** zeigt Einträge von Geräteprotokollen an. *Das Geräteprotokoll dient nur für Kaseya Support-Zwecke.* Das Geräteprotokoll zeigt die tatsächlichen Nachrichten an, die zwischen VSA und einem ausgewählten Gerät hin- und her gesendet wurden. Da Dienstanbieter diese Informationen nicht benötigen, werden Geräteprotokolle für ein ausgewähltes Gerät nur angezeigt, wenn die Schaltfläche **Protokoll anfordern** auf der Seite **Geräteübersicht** angeklickt wird. Einträge von Geräteprotokollen werden dann in der Registerkarte **Protokolle** angezeigt. Durch Klicken auf die Schaltfläche **Protokolldetails anzeigen** bei einem bestimmten Protokolleintrag wird der Text der Nachricht angezeigt.

Gerät-Nachrichten

Mobile > Vorgänge > Gerät-Nachrichten

Die Seite **Gerät-Nachrichten** erstellt und sendet Nachrichten, die auf ausgewählten mobilen Geräten als Pop-up-Nachrichten angezeigt werden. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Nachricht senden** – Zeigt ein Dialogfenster zur Eingabe einer Textnachricht an. Klicken Sie auf die Schaltfläche **Nachricht senden**, um die Nachricht an ein ausgewähltes Gerät zu senden.
- **Nachricht erneut senden** – Sendet eine ausgewählte Nachricht erneut.
- **Entfernen** – Entfernt eine ausgewählte Nachricht.
- **Aktualisieren** – Aktualisiert die Seite.

Gerätetabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - - Erstellt
  - - Einladung fehlgeschlagen
  - - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - - Einladung abgelehnt
  - - Installation läuft
  - - Installation fehlgeschlagen
  - - Normal – Die Anwendung ist installiert und funktioniert normal.
  - - Befehl ausstehend
  - - Befehl gesendet
  - - Keine Antwort
  - - Wird verarbeitet
  - - Befehl gesendet – erneut versuchen
  - - Abmelden
  - - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - - Android
  - - Apple
  - - Blackberry
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Besitzer** – Der Eigentümer des Geräts.

Nachrichtentabellenspalten

- **Richtung der Nachricht** –
  - - vom Gerät gesendet
  - - vom VSA-Administrator gesendet
- **Nachrichten-Datum** – Datum/Uhrzeit der Nachricht.
- **Von** – *Gilt nur für Gerät-Nachrichten.* Der Gerätebezeichner und die Rechnergruppe.
- **Meldung** – Der Text der Nachricht.

Verlorene Geräte

Mobile > Vorgänge > Verlorene Geräte

Auf der Seite **Verlorene Geräte** wird ein Gerät als verloren oder gefunden gekennzeichnet und es werden die Aktionen eingestellt, die durchgeführt werden können, wenn ein Gerät verloren oder gestohlen wurde. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Gerät als verloren markieren** – Kennzeichnet das Gerät als verloren.
- **Gerät als gefunden markieren** – Kennzeichnet das Gerät als gefunden.

- **Nachricht senden** – Sendet eine Nachricht an das Gerät.
- **Gerät sperren** – Bei Markierung wird das Gerät gesperrt und der Benutzerzugriff verhindert.
- **Gestohlenalarm auf Gerät auslösen** – Bei Markierung sagt das Gerät bei jedem Einschalten "Dieses Telefon ist gestohlen". Dieser Alarm kann durch Löschen des Geräts deaktiviert werden.
- **Gerät löschen** – Bei Markierung wird das Gerät auf seine Standardeinstellungen zurückgesetzt. Beim Löschen eines Geräts werden alle Benutzerdaten gelöscht, einschließlich der Management-Anwendung/Kaseya Agent-Anwendung. Die Kaseya Agent-Anwendung kann sich nach dem Löschen des Geräts nicht mehr anmelden.
- **Passcode löschen** – Setzt Passcodes auf verwalteten iOS-Geräten zurück. Durch ein Zurücksetzen wird das Gerät entsperrt, wodurch der Benutzer das Gerät entweder ohne Passcode verwenden oder einen neuen Passcode einstellen kann. Durch Löschen des Passcodes wird nicht das darunterliegende Sicherheitsprofil geändert. Wenn das Gerät so konfiguriert ist, dass ein Passcode erforderlich ist, so wird der Benutzer direkt dazu aufgefordert, einen neuen einzugeben.
- **Aktualisieren** – Aktualisiert die Seite.

Tabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.

  (leer) - Nachverfolgung ist nicht aktiviert.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Verloren** – Bei Markierung wurde das Gerät als verloren oder gestohlen gekennzeichnet.
- **Löschen** – Bei Markierung wurde das Gerät gelöscht, d. h. auf seine Standardeinstellungen zurückgesetzt. Beim Löschen eines Geräts werden alle Benutzerdaten gelöscht.

- **Sperren** – Bei Markierung wird das Gerät gesperrt und der Benutzerzugriff verhindert.
- **Alarm auf Gerät auslösen** – Bei Markierung sagt das Gerät bei jedem Einschalten "Dieses Telefon ist gestohlen", es sei denn, es wird gelöscht und somit auf seine Standardeinstellungen zurückgesetzt. Beim Löschen eines Geräts werden alle Benutzerdaten gelöscht.

Kontakte

Mobile > Vorgänge > Kontakte

Die Seite **Kontakte** sichert Kontaktlisten von Geräten und stellt sie wieder her. Wenn ein Gerät verloren oder gestohlen ist, kann die Kontaktliste auf einem neuen Gerät wiederhergestellt werden. Eventuell muss eine Kontaktliste auch auf einem vorhandenen Gerät wiederhergestellt werden, wenn das Gerät gelöscht (zurückgesetzt) wird und alle Benutzerdaten gelöscht werden. Wenn mehrere Sicherungen vorhanden sind, können Sie die anzuzeigende Sicherung auswählen. Wenn eine Sicherung ausgewählt wird, werden die Namen der Kontakte rechts auf der Seite aufgeführt. Durch Klicken auf einen Namen werden die verfügbaren Informationen für diesen Kontakt angezeigt: E-Mails, Adressen, Telefonnummern und Anmerkungen. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Jetzt sichern** – Sichert die Kontaktliste eines ausgewählten Geräts sofort.
- **Wiederherstellen** – Stellt die Kontaktliste von ausgewählten Geräten wieder her. Ein Dialogfenster wird angezeigt und Sie können die Sicherung auswählen, die Sie wiederherstellen möchten.
- **Löschen** – Löscht die Kontaktliste von ausgewählten Geräten.
- **Aktualisieren** – Aktualisiert die Seite.
- **Backup** – Wählt die rechts auf der Seite anzuzeigenden Kontakte aus.

Gerätetabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple

- Blackberry

- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.
  (leer) - Nachverfolgung ist nicht aktiviert.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Anzahl Backups** – Anzahl der erstellten Sicherungen.
- **Datum letztes Backup** – Datum/Uhrzeit der letzten Sicherung.
- **Datum letzte Wiederherstellung** – Datum/Uhrzeit der letzten Wiederherstellung.

Anwendungsprotokolle

Mobile > Vorgänge > Anwendungsprotokolle

Die Seite **Anwendungsprotokolle** zeigt ein Protokoll der Aktivität der **Mobile Device Management**-Anwendung an nach:

- **Ereignis-ID**
- **Ereignisname**
- **Meldung**
- **Admin**
- **Ereignis-Datum**

Wenn Informationen unerwartet geändert oder entfernt wurden, prüfen Sie diese Seite, um zu ermitteln, welche Ereignisse und Administratoren möglicherweise beteiligt waren.

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#6875.htm)*.

Protokollierte Ereignisse umfassen Folgendes:

Gerät sichern
Servereinstellungen ändern
Systemeinstellungen ändern
Passcode löschen
Gerät erstellen
Gerät erstellt
Profil löschen
Gerät gelöscht
Gerät gefunden
Gerät gefunden
Einladung erneut gesendet
Gerät sperren
Verlorenes Gerät
Befehle als abgeschlossen kennzeichnen
Benachrichtigung bearbeiten
Check-in anfordern
Check-in anfordern
Protokolle anfordern
Gerät wiederherstellen
Audit starten
Geplanter Audit
Alarm auf Gerät auslösen

Geräteverfolgung starten
Geräteverfolgung anhalten
Gerät aktualisiert
Gerät löschen

Mehrere Geräte lokalisieren

Mobile > Standort > Mehrere Geräte lokalisieren

Die Seite **Mehrere Geräte lokalisieren** zeigt den aktuellen Standort von einem oder mehreren ausgewählten Geräten auf einer Karte an. Jede nummerierte Markierung auf der Karte bezieht sich auf eine nummerierte Liste auf der rechten Kartenseite. Die nummerierte Liste gibt den Namen jedes Geräts, seine Telefonnummer und wann es zuletzt seinen Standort angegeben hat an. Die Anzeige der Daten wird anhand eines bestimmten Startdatums und Uhrzeit gefiltert. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Hinweis: Wenn Sie keine Standortmarkierung eines Geräts sehen, das Sie nachverfolgen, versuchen Sie, den Filter zurückzusetzen, sodass ein früherer Datumsbereich angezeigt wird.

Aktionen

- **Aktuellen Standort abrufen** – Gibt den aktuellen Standort des Geräts auf Anfrage aus, aber verfolgt ihn nicht kontinuierlich nach. Der letzte Standort eines Geräts – abgerufen entweder durch den Befehl **Aktuellen Standort abrufen** oder durch Starten der Nachverfolgung – wird auf einer Karte durch **Mehrere Geräte lokalisieren** *(siehe 22)* angezeigt.
- **Nachverfolgung starten** – Startet die Standortnachverfolgung des Geräts. Nach dem Start können Sie das Gerät auf einer Karte mithilfe von **Ein einziges Gerät nachverfolgen** *(siehe 23)* nachverfolgen.
- **Nachverfolgung anhalten** – Hält die Standortnachverfolgung des Geräts an.
- **Standortverlauf** – Zeigt den Standortverlauf eines Geräts an. Standortdaten werden sowohl durch die Befehle **Aktuellen Standort abrufen** als auch durch Nachverfolgung des Geräts ausgegeben.

Verwenden der Karte

1. Wählen Sie ein oder mehrere Geräte im mittleren Fensterbereich aus.
2. **Datum und Zeit** – Ändern Sie bei Bedarf den Datums- und Zeitfilter. Der Filter begrenzt die Anzeige der Gerätestandorte ab einem bestimmten Startdatum und Uhrzeit.
3. **Aktualisieren** – Aktualisieren Sie die Karte nach Zurücksetzen des Filters **Datum und Zeit**.

Gerätetabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet

- Keine Antwort
- Wird verarbeitet
- Befehl gesendet – erneut versuchen
- Abmelden
- Befehl gesendet – fehlgeschlagen

- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.
  (leer) - Nachverfolgung ist nicht aktiviert.
- **Daten** – Bei Markierung verfügt das Gerät über Standortdaten.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefon** – Die Telefonnummer des Geräts.
- **Besitzer** – Der Eigentümer des Geräts.
- **Anzahl** – Anzahl der nachverfolgten Standorte.

Ein einziges Gerät nachverfolgen

Mobile > Standort > Ein einziges Gerät nachverfolgen

Die Seite **Ein einziges Gerät nachverfolgen** zeigt Standortverfolgungsdaten für ein ausgewähltes Gerät an. Jede nummerierte Markierung auf der Karte bezieht sich auf eine nummerierte Liste auf der rechten Kartenseite. Die nummerierte Liste gibt Datum und Zeit an, wann sich das Gerät an dem Ort befunden hat. Die Datenanzeige wird durch einen bestimmten Datums- und Uhrzeitbereich gefiltert. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

> **Hinweis:** Wenn Sie keine Standortmarkierung eines Geräts sehen, das Sie nachverfolgen, versuchen Sie, den Filter zurückzusetzen, sodass ein früherer Datumsbereich angezeigt wird.

Aktionen

- **Aktuellen Standort abrufen** – Gibt den aktuellen Standort des Geräts auf Anfrage aus, aber verfolgt ihn nicht kontinuierlich nach. Der letzte Standort eines Geräts – abgerufen entweder durch den Befehl **Aktuellen Standort abrufen** oder durch Starten der Nachverfolgung – wird auf einer Karte durch **Mehrere Geräte lokalisieren** *(siehe 22)* angezeigt.
- **Nachverfolgung starten** – Startet die Standortnachverfolgung des Geräts. Nach dem Start können Sie das Gerät auf einer Karte mithilfe von **Ein einziges Gerät nachverfolgen** *(siehe 23)* nachverfolgen.
- **Nachverfolgung anhalten** – Hält die Standortnachverfolgung des Geräts an.
- **Standortverlauf** – Zeigt den Standortverlauf eines Geräts an. Standortdaten werden sowohl durch die Befehle **Aktuellen Standort abrufen** als auch durch Nachverfolgung des Geräts ausgegeben.

Verwenden der Karte

1. Wählen Sie ein einzelnes Gerät aus dem mittleren Fensterbereich aus.

2. **Datum und Zeit** – Ändern Sie bei Bedarf den Datums- und Zeitfilter. Der Filter begrenzt die Anzeige der Gerätestandorte auf einen Datums- und Uhrzeitbereich.
3. **Aktualisieren** – Aktualisieren Sie die Karte nach Zurücksetzen des Filters **Datum und Zeit**.

Tabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.

  (leer) - Nachverfolgung ist nicht aktiviert.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Besitzer** – Der Eigentümer des Geräts.
- **Anzahl** – Anzahl der nachverfolgten Standorte.

App-Profile

Mobile > Anw.-Management > App-Profile

Die Seite **App-Profile** definiert Anwendungsprofile. App-Profile bestimmen, welche Anwendungen auf verwalteten mobilen Geräten installiert werden müssen bzw. nicht installiert werden dürfen. Jedes App-Profil stellt eine andere Kombination aus Anwendungen dar. Alle Anwendungen, die zum selben App-Profil gehören, sind entweder erforderlich oder nicht zugelassen. Sie können einem einzigen mobilen Geräte mehrere App-Profile zuweisen. Änderungen an einem Profil betreffen alle Geräte, die diesem App-Profil zugewiesen sind. Verwalteten mobilen Geräten wird ein App-Profil über Mobile>**App-Profile zuweisen** *(siehe 26)* zugewiesen.

- Wenn eine Anwendung nicht zugelassen ist, deinstalliert Mobile Device Management diese Anwendung nicht automatisch. Der Benutzer wird dazu aufgefordert, die Deinstallation manuell vorzunehmen.
- Wenn eine Anwendung erforderlich ist und es sich um eine *Store-App* handelt, sendet Mobile Device Management eine Einladung mit einem Link zur Installation der Anwendung an den Gerätebenutzer. Wenn eine Anwendung erforderlich ist und es sich um eine *Unternehmens-App* handelt, so wird sie automatisch per Push-Vorgang auf das Gerät übertragen. Weitere Informationen zu diesen beiden Arten von Anwendungen finden Sie unter **Artikel aus Haupt-App-Katalog hinzufügen** *(siehe 27)*.

Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Neu** – **Fügt ein neues App-Profil hinzu** *(siehe 25)*.
- **Bearbeiten** – **Bearbeitet ein ausgewähltes App-Profil** *(siehe 25)*.
- **Löschen** – Löscht ein ausgewähltes App-Profil.
- **Apps aus Hauptkatalog hinzufügen** – Fügt Anwendungen aus dem **App-Katalog** *(siehe 26)* zu einem ausgewählten App-Profil hinzu.
- **Entfernen** – Entfernt eine ausgewählte Anwendung aus einem ausgewählten App-Profil.

Tabellenspalten von App-Profilen

- **Betriebssystem**
  - Android
  - Apple
- **Typ** – Typ des App-Profils.
  - Nicht zugelassen
  - Erforderlich
- **Name** – Der Name des App-Profils.

Anwendungstabellenspalten

- **(App-Typ)**
  - **Store-App** – Bei Auswahl muss eine URL **angegeben werden.**
  - **Unternehmens-App** – Bei Auswahl muss eine App-Programmdatei **angegeben werden.**
- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.

App-Profil hinzufügen / bearbeiten

Mobile > Anw.-Management > App-Profile > Neu / App-Profil bearbeiten

Das Dialogfenster **Hinzufügen / App-Profil** gibt ein App-Profil an. Ein App-Profil bestimmt, welche Anwendungen auf verwalteten mobilen Geräten installiert werden müssen bzw. nicht installiert werden dürfen.

- **Name** – Der Name des Anwendungsprofils.
- **Typ** – Legt die Regel für alle Anwendungen fest, die diesem App-Profil zugewiesen sind.
  - `Required` - Anwendungen, die diesem App-Profil hinzugefügt werden, müssen auf dem verwalteten mobilen Gerät installiert werden.

- `Disallowed` - Anwendungen, die diesem App-Profil hinzugefügt werden, werden nicht auf dem verwalteten mobilen Gerät installiert.
- **Betriebssystem** - `Android` oder `iOS`.

App-Profile zuweisen

Mobile > Anw.-Management > App-Profile zuweisen

Die Seite **App-Profile zuweisen** weist mobile Geräte ausgewählten Anwendungsprofilen zu. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Aktionen

- **Zuweisen** – Weist ausgewählte mobile Geräte ausgewählten App-Profilen zu.
- **Entfernen** – Entfernt ausgewählte App-Profile von ausgewählten mobilen Geräten.

Gerätetabellenspalten

- **Nachverfolgen**
  - Die Nachverfolgung wurde gestartet und das Gerät ist angemeldet.
  - Die Nachverfolgung steht noch aus und beginnt, wenn sich das Gerät anmeldet.
  (leer) - Nachverfolgung ist nicht aktiviert.
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.

Tabellenspalten von App-Profilen

- **Betriebssystem**
  - Android
  - Apple
- **Typ** – Typ eines App-Profils.
  - Nicht zugelassen
  - Erforderlich
- **Name** – Der Name des App-Profils.

App-Katalog

Mobile > Anw.-Management > App-Katalog

Die Seite **App-Katalog** enthält einen Katalog der App-Elemente. Jedes App-Element identifiziert eine einzelne Anwendung eindeutig, die auf einem mobilen Gerät erforderlich bzw. nicht zugelassen ist. Nach dem Hinzufügen zum Katalog können App-Elemente dann zu **App-Profilen** *(siehe 24)* hinzugefügt werden. Ein App-Profil ist eine Liste von App-Elementen, die bestimmt, welche Anwendungen auf verwalteten mobilen Geräten erforderlich bzw. nicht zugelassen sind.

Aktion

- **Hinzufügen** – Erstellt ein neues App-Element im **App-Katalog**.
- **Bearbeiten** – Bearbeitet ein ausgewähltes App-Element im **App-Katalog**.
- **Löschen** – Löscht ein ausgewähltes App-Element aus dem **App-Katalog**.
- **Installationseinladung senden** – Sendet eine Nachricht, die den Benutzer dazu einlädt, eine Anwendung auf dem mobilen Gerät des Benutzers zu installieren.

Tabellenspalten

- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.
- **Geräte-BS** - `Android` oder `iOS`.
- **App-Typ** – Gibt an, ob die Anwendung von einem App-Store installiert oder von VSA als Unternehmens-App heruntergeladen wird.
  - **Store-App** – Bei Auswahl muss eine URL **angegeben werden**.
  - **Unternehmens-App** – Bei Auswahl muss eine App-Programmdatei **hochgeladen werden.**
- **URL** – Gibt die URL an, die mobile Geräte nutzen, um die Anwendung aus dem App-Store herunterzuladen.
- **App-Programmdatei** – Gibt ein App-Bündel zum Hochladen auf VSA an. Das App-Bündel ist entweder eine Android `.apk`-Datei oder eine iOS `.ipa`-Datei. Nach dem Hochladen verwaltet VSA die Verteilung der Anwendung auf verwalteten mobilen Geräten.

Artikel aus Haupt-App-Katalog hinzufügen

Mobile > Anw.-Management > App-Katalog > Artikel aus Haupt-App-Katalog hinzufügen

Das Dialogfenster **Artikel aus Haupt-App-Katalog hinzufügen** identifiziert eine einzelne Anwendung eindeutig, die auf einem verwalteten mobilen Gerät installiert werden kann oder nicht zugelassen ist. Die ersten vier Werte **müssen genau den Werten entsprechen, die bei einem Anwendungsaudit des mobilen Geräts ausgegeben werden.**

- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.
- **Geräte-BS** - `Android` oder `iOS`.
- **App-Typ** – Gibt an, ob die Anwendung von einem App-Store installiert oder von VSA als Unternehmens-App heruntergeladen wird.
  - **Store-App –** Bei Auswahl muss eine URL **angegeben werden.**
  - **Unternehmens-App** – Bei Auswahl muss eine App-Programmdatei **angegeben werden.**
- **URL** – Gibt die URL an, die mobile Geräte nutzen, um die Anwendung aus dem App-Store herunterzuladen.
- **App-Programmdatei** – Gibt ein App-Bündel zum Hochladen auf VSA an. Das App-Bündel ist entweder eine Android `.apk`-Datei oder eine iOS `.ipa`-Datei. Nach dem Hochladen verwaltet VSA die Verteilung der Anwendung auf verwalteten mobilen Geräten.

App-Bestand

Mobile > Anw.-Management > App-Bestand

Die Seite **App-Bestand** erzeugt eine Liste von App-Elementen anhand der Anwendungen, die auf den verwalteten mobilen Geräten ermittelt wurden. Anstatt App-Elemente manuell im App-Katalog anzugeben, können Sie ein von **App-Bestand** automatisch erzeugtes App-Element dem **App-Katalog** hinzufügen. Die Liste der Geräte, die in **App-Bestand** angezeigt werden, hängt vom Geräte-ID- / Rechner-Gruppenfilter ab.

Aktionen

- **Zum App-Katalog hinzufügen** – Fügt ausgewählte App-Elemente zum **App-Katalog** *(siehe 26)* hinzu.
- **Nachricht senden** – Zeigt ein Dialogfenster zur Eingabe einer Textnachricht an. Klicken Sie auf die Schaltfläche **Nachricht senden**, um die Nachricht an ein ausgewähltes Gerät zu senden.

Tabellenspalten

- **Betriebssystem** - `Android` oder `iOS`.
- **Paketname** – Der vollständige Name der Anwendung im Reverse-Domain-Format. Beispiel: `com.kaseya.enterprise.agent`.
- **App-Name** – Der Anzeigename der Anwendung. Beispiel: `Agent`.
- **Version** – Die Versionsnummer der Anwendung. Beispiel: `1.2.0.0`.

Profile erstellen

Mobile > Profile > Profile erstellen

Die Seite **Profile erstellen** definiert Konfigurationsprofile. Profile legen fest, wie Geräte konfiguriert und mit **Mobile Device Management** verwaltet werden. Jedes Profil stellt eine andere Kombination aus Optionen dar. Änderungen an einem Profil betreffen alle Geräte, die diesem Profil zugewiesen sind. Ein Profil wird Geräten mit Mobile > **Profile zuweisen** *(siehe 36)* zugewiesen.

Profiltypen

- **E-Mail-Profil** *(siehe 29)* – Konfiguriert den E-Mail-Client auf einem verwalteten mobilen Gerät. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.
- **Sicherheitsprofil** *(siehe 30)* – Konfiguriert Richtlinien in Bezug auf die Erstellung von PINs. PINs werden von Gerätebenutzern verwendet, um ihre Geräte zu entsperren.
- **Web Clip-Profil** *(siehe 31)* – Gibt eine Webanwendungsverknüpfung zu einer URL an, auf die das Gerät zugreifen kann. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden
- **iOS 4 Geräte-Funktionsprofil** *(siehe 31)* – Gilt für iOS-Geräte mit einer Version unter iOS 5. Aktiviert und deaktiviert beliebte Funktionen auf Geräten mit iOS 4.
- **iOS-Geräte-Funktionsprofil** *(siehe 32)* – Gilt nur für iOS5, iOS6, iOS7. Aktiviert und deaktiviert beliebte Funktionen auf iOS-Geräten.
- **Geräteort und Tracking-Profil** *(siehe 34)* – Stellt Anmeldungs- und Standortoptionen auf Geräten ein. Dies ist das einzige Profil, das für Blackberrys gilt.
- **Benutzerdefiniertes iOS-Konfigurationsprofil** *(siehe 33)* – Ein Profil, das mithilfe des **iPhone-Konfigurationsprogramms** *(http://support.apple.com/kb/DL1466)* erstellt und in **Mobile Device Management** importiert wurde.

- **WiFi-Profil** *(siehe 35)* – Stellt die WiFi-Optionen auf Geräten ein. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.

Aktionen

- **Neu** – Fügt ein neues Profil hinzu.
- **Bearbeiten** – Bearbeitet ein ausgewähltes Profil.
- **Löschen** – Löscht ein ausgewähltes Profil.

E-Mail-Profil

Mobile > Profile > Profile erstellen > Neu/Bearbeiten > E-Mail-Profil

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Falls die Felder für Benutzeranzeigename, E-Mail-Adresse, Benutzername oder Kennwort leer sind, werden sie aus dem Gerätedatensatz ausgefüllt.
- Dieser Profiltyp wird teilweise auf Android-Geräten unterstützt.
- Dieser Profiltyp wird nicht auf Blackberry-Geräten unterstützt.

Das **E-Mail-Profil** konfiguriert den E-Mail-Client auf einem verwalteten mobilen Gerät. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.

- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Kontotyp** – `IMAP`, `POP`, `Gmail` oder `Exchange`. Die `Gmail`-Option ist eine vordefinierte IMAP-Konfiguration eines Gmail-Kontos. Nur die Felder "Benutzername" und "Kennwort" müssen ausgefüllt werden, um diese `Gmail`-IMAP-Konfiguration abzuschließen. Siehe **Konfigurieren eines Exchange E-Mail-Profils** unten.
- **Benutzeranzeigename** – Der Anzeigename des E-Mail-Kontos.

> **Hinweis:** Wenn bei iOS die Felder **Benutzeranzeigename** und **E-Mail-Adresse** leer gelassen werden, wird der Gerätebenutzer dazu aufgefordert, seinen Benutzernamen und seine E-Mail-Adresse einzugeben, wenn das Profil auf dem Gerät angewendet wird.

- **E-Mail-Adresse** – Die E-Mail-Adresse des Benutzers.
- **Eingehende Server-IP oder Hostname** – Der IMAP- oder POP3-Eingangsserver. Zum Beispiel `pop.youremail.com` oder `imap.youremailserver.com`.
- **Eingehender Server-Port** – Die vom eingehenden E-Mail-Dienst verwendete Port-Nummer. Bei POP3 in der Regel `110` oder bei aktiviertem SSL `995`. Wenn IMAP aktiviert ist, in der Regel `143` oder bei aktiviertem SSL `993`.
- **Kennwort für Eingangsserver erforderlich** – Bei Markierung ist für den Eingangsserver ein Kennwort erforderlich.
  - **Kennwort für Eingangsserver** – Geben Sie das Kennwort ein.
- **SSL für eingehende E-Mail verwenden** – Bei `Yes` wird die Kommunikation mit dem Eingangsserver mithilfe von SSL verschlüsselt. Damit diese Funktion verwendet werden kann, muss Ihr Eingangsserver SSL unterstützen.
- **Nachrichten auf dem Server belassen** – Bei `Yes` bleiben die E-Mails auf dem Eingangsserver gespeichert, nachdem sie auf das Gerät übertragen wurden.
- **Ausgangsserver-IP oder Hostname** – Der SMTP-Ausgangsserver. Zum Beispiel `smtp.youremailserver.com`.
- **Ausgangsserver-Port** – Die Port-Nummer, die der Ausgangsserver verwendet. In der Regel `25` oder bei aktiviertem SSL `465`.
- **Benutzername für Ausgangsserver** – Wenn "Ausgangs-Authentifizierung" markiert ist, der Benutzername für den Ausgangsserver.

- **Gleiches Kennwort wie für Eingangsserver verwenden** – Bei Markierung verwenden sowohl Eingangs- als auch Ausgangsserver das gleiche Eingangskennwort. Geben Sie ein Kennwort an, falls dieses Feld leer ist.
  - **Ausgangsserver-Passwort** – Geben Sie ein Kennwort ein.
- **SSL für ausgehende E-Mail verwenden** – Bei `Yes` wird die Kommunikation mit dem Ausgangsserver mithilfe von SSL verschlüsselt. Damit diese Funktion verwendet werden kann, muss Ihr Ausgangsserver SSL unterstützen.

Konfigurieren eines Exchange E-Mail-Profils

Stellen Sie folgende Werte ein, um ein Exchange E-Mail-Profil in **Mobile Device Management** zu konfigurieren:

- **Kontotyp** – Wählen Sie `Exchange`.
- **E-Mail-Adresse** – Geben Sie eine E-Mail-Adresse ein.
- **Eingehende Server-IP oder Hostname** – Geben Sie den Exchange-Serverhostnamen ein.
- **Benutzername für Eingangsserver** – Geben Sie einen Domain-Benutzernamen ein im Format `domain\username`
- **Kennwort für Eingangsserver erforderlich** – Markieren Sie dieses Kontrollkästchen.
- **Kennwort** – Geben Sie das Kennwort für den Domain-Benutzernamen ein.
- **Eingehender Server-Port** – Standardeinstellungen auf `143`.
- **Ausgangsserver-Port** – Standardeinstellungen auf `25`.
- **SSL für eingehende E-Mail verwenden** – Als Standardeinstellung markiert.
- **Gleiches Kennwort wie für Eingangskennwort verwenden** – Markieren Sie dieses Kontrollkästchen.

Hinweis: *Nur für Geräte mit iOS*: Wenn Sie Benutzername, E-Mail-Adresse und Kennwort in einem Exchange E-Mail-Profil leer lassen, müssen Sie das Profil mithilfe des iPhone-Konfigurationsprogramms anwenden. Ansonsten müssen Sie in **Mobile Device Management** für jedes iOS-E-Mail-Profil getrennte Profile erstellen und Benutzernamen, E-Mail-Adresse und Kennwort angeben.

Sicherheitsprofil

Mobile > Profile > Profile erstellen >Neu/Bearbeiten > Sicherheitsprofil

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Dieser Profiltyp wird teilweise auf Android-Geräten unterstützt. Unterstützte Felder sind: Simple zulassen, PIN erzwingen, Max. gescheiterte Versuche, Max. Inaktivität, Mindestlänge, Alphanumerisch erforderlich
- Dieser Profiltyp wird nicht auf Blackberry-Geräten unterstützt.

Das **Sicherheitsprofil** konfiguriert Richtlinien in Bezug auf die Erstellung von PINs. PINs werden von Gerätebenutzern verwendet, um ihre Geräte zu entsperren.

Hinweis: Android unterstützt nur die folgenden Einstellungen: Simple zulassen, PIN erzwingen, Mindestlänge, Alphanumerisch erforderlich, Max. Inaktivität und Max. gescheiterte Versuche.

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Simple zulassen** – Bei Markierung darf der Benutzer aufeinanderfolgende oder sich wiederholende Zeichen in seinen Passcodes verwenden. So sind zum Beispiel die Passcodes `3333` oder `DEFG` erlaubt.
- **PIN erzwingen** – Bei Markierung muss der Benutzer eine PIN angeben. Wenn diese Option nicht markiert ist, ist kein Kennwort erforderlich.

- **Max. gescheiterte Versuche** – Legt fest, wie viele gescheiterte Versuche zur PIN-Eingabe vorgenommen werden können, bevor das Gerät gelöscht wird. Die Standardeinstellung hängt vom Gerätehersteller ab.
- **Max. Inaktivität** – Die Wartezeit in Sekunden bis zum Sperren des Geräts, während der ein Benutzer das Gerät nicht verwendet.
- **Max. PIN-Alter in Tagen** – Die maximale Anzahl der Tage, an denen dieselbe PIN verwendet wird.
- **Min. komplexe Zeichen** – Die Mindestanzahl komplexer Zeichen, die in einer PIN erforderlich sind.
- **Mindestlänge** – Die erforderliche Mindestlänge für eine PIN.
- **Alphanumerisch erforderlich** – Bei Markierung sind sowohl Buchstaben als auch Zahlen erforderlich.
- **PIN-Historie** – Bei Markierung wird ein PIN-Verlauf aufgezeichnet.
- **Manueller Abruf beim Roaming** – Wenn leer, werden Geräte während des Roaming nur dann synchronisiert, wenn ein Benutzer auf das Konto zugreift.
- **Max. Aufschub** – Gibt an, wie schnell das Gerät nach der Verwendung entsperrt werden kann, ohne dass erneut die PIN eingegeben werden muss.

Web Clip-Profil

Mobile > Profile > Profile erstellen > Neu/Bearbeiten > Web Clip-Profil

- Dieser Profiltyp wird auf iOS-Geräten unterstützt. Bei iOS-Geräten muss die URL mit HTTP oder HTTPS beginnen
- Dieses Profil wird nicht auf Android- und Blackberry-Geräten unterstützt.

Das **Web Clip-Profil** gibt eine Webanwendungsverknüpfung zu einer URL an, auf die das Gerät zugreifen kann. Ein Unternehmen kann Verknüpfungen auf Geräten installieren, die direkt zu seinen Websites oder Supportdokumenten führen. Einem Gerät können mehrere Profile zugewiesen werden, wobei für jedes **Web Clip-Profil** eine Verknüpfung definiert ist. Gilt derzeit nur für iOS-Geräte.

Tabellenspalten

- **Name** – Der Name des Profils.
- **Beschreibung** – Die Beschreibung des Profils.
- **URL** – Die URL der Webanwendungsverknüpfung.
- **Bezeichnung** – Ein Anzeigename für die Webanwendungsverknüpfung.
- **Symbol** – Lädt eine png-Datei hoch, die als Symbol für die Verknüpfung dient.
- **Ist entfernbar** – Bei Markierung kann der Benutzer die Webanwendungsverknüpfung löschen.

Geräte-Funktionsprofil iOS 4

Mobile > Profile > Profile erstellen > Neu/Bearbeiten > Geräte-Funktionsprofil iOS 4

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Dieses Profil wird nicht auf Android- und Blackberry-Geräten unterstützt.

Mit dem **Geräte-Funktionsprofil iOS 4** werden beliebte Funktionen auf iOS-Geräten aktiviert und deaktiviert. Gilt für iOS-Geräte mit einer Version unter iOS 5.

Tabellenspalten

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Anwendungsinstallation zulassen** – Bei Markierung dürfen Anwendungen installiert werden.
- **Kamera zulassen** – Bei Markierung ist die Kamera des Geräts aktiviert.

- **Anstößige Inhalte zulassen** – Bei Markierung wird die Filterung von explizitem Inhalt deaktiviert.
- **Screenshot zulassen** – Bei Markierung kann das Gerät Momentaufnahmen seines Bildschirms erstellen.
- **YouTube zulassen** – Bei Markierung ist YouTube aktiviert.
- **iTunes zulassen** – Bei Markierung ist iTunes aktiviert.
- **Safari zulassen** – Bei Markierung ist der Safari-Webbrowser aktiviert.

iOS-Geräte-Funktionsprofil

Mobile > Profile > Profile erstellen > Neu/Bearbeiten > iOS-Geräte-Funktionsprofil

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Dieses Profil wird nicht auf Android- und Blackberry-Geräten unterstützt.

Mit dem **iOS-Geräte-Funktionsprofil** werden beliebte Funktionen auf Geräten mit iOS 5 und höher aktiviert und deaktiviert.

Tabellenspalten

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Anwendungsinstallation zulassen** – Bei Markierung dürfen Anwendungen installiert werden.
- **Kamera zulassen** – Bei Markierung ist die Kamera des Geräts aktiviert.
- **Anstößige Inhalte zulassen** – Bei Markierung wird die Filterung von anstößigem Inhalt deaktiviert.
- **Screenshot zulassen** – Bei Markierung kann das Gerät Momentaufnahmen seines Bildschirm erstellen.
- **YouTube zulassen** – Bei Markierung ist YouTube aktiviert.
- **iTunes zulassen** – Bei Markierung ist iTunes aktiviert.
- **Safari zulassen** – Bei Markierung ist der Safari-Webbrowser aktiviert.
- **Face Time zulassen** – Bei Markierung können Benutzer Videoanrufe über Face Time tätigen und annehmen.
- **Automatisches Synchronisieren beim Roaming zulassen** – Bei Markierung synchronisieren sich Geräte während des Roaming. Wenn nicht markiert, werden Geräte nur dann synchronisiert, wenn ein Benutzer auf das Konto zugreift.
- **Siri zulassen** – Bei Markierung können Benutzer Siri, Sprachbefehle oder Diktat verwenden.
- **Sprachwahl zulassen** – Bei Markierung können Benutzer durch Sprachbefehle wählen.
- **In-App Purchase zulassen** – Bei Markierung können Benutzer In-App-Käufe vornehmen.
- **Eingabe des Benutzerkennworts für iTunes Store bei allen Einkäufen erzwingen** – Bei Markierung müssen Benutzer vor dem Einkaufen ihr Apple-ID-Kennwort eingeben. Normalerweise gibt es eine kurze Aufschubzeit nach einem Einkauf, bevor Benutzer sich für weitere Einkäufe erneut authentifizieren müssen.
- **Multiplayer-Spiele zulassen** – Bei Markierung können Benutzer Multiplayer-Spiele im Game Center spielen.
- **Hinzufügen von Game Center-Freunden zulassen** – Bei Markierung können Benutzer Freunde im Game Center hinzufügen.
- **Automat. Ausfüllen aktivieren** – Bei Markierung speichert Safari Eingaben in Webformulare.
- **Betrugswarnung erzwingen** – Bei Markierung warnt Safari Benutzer, wenn besuchte Websites als betrügerisch oder gefährlich eingestuft werden.
- **JavaScript aktivieren** – Bei Markierung führt Safari JavaScript auf Websites aus.
- **Pop-ups blockieren** – Bei Markierung ist die Pop-up-Blockierungsfunktion von Safari aktiviert.

- **Cookies zulassen** – Wählen Sie aus, wann Cookies zugelassen werden sollen: `Never`, `From visited sites`, `Always`.
- **Backups zulassen** – Bei Markierung können Benutzer ihr Gerät in iCloud sichern.
- **Dokumentsynchronisierung zulassen** – Bei Markierung können Benutzer Dokumente in iCloud speichern.
- **Photo-Stream zulassen (Deaktivieren kann Datenverlust zur Folge haben)** – Bei Markierung können Benutzer Fotostream aktivieren.

> **Warnung:** Wenn nicht aktiviert, löscht dieses Profil Fotostream-Fotos vom Benutzergerät und verhindert, dass Fotos von Camera Roll nach Fotostream gesendet werden. Wenn es keine anderen Kopien dieser Fotos gibt, können sie verloren gehen.

- **Senden von Diagnosedaten an Apple zulassen** – Bei Markierung werden iOS-Diagnosedaten an Apple gesendet.
- **Zulassen, dass Nutzer nicht vertrauenswürdige TLS-Zertifikate akzeptiert** – Bei Markierung werden Benutzer gefragt, ob sie Zertifikaten vertrauen möchten, die nicht verifiziert werden können. Diese Einstellung gilt für Safari und E-Mail-, Kontakt- und Kalenderkonten.
- **Verschlüsselte Backups erzwingen** – Wenn nicht markiert, dann kann der Benutzer in iTunes auswählen, ob eine Sicherung vom Gerät auf einen lokalen Rechner verschlüsselt werden soll oder nicht. Bei Markierung wird der Benutzer dazu gezwungen, die Sicherung zu verschlüsseln. Wenn eine Sicherung verschlüsselt wird, wird der Benutzer durch ein Textfeld auf dem Gerät dazu aufgefordert, ein Verschlüsselungskennwort einzugeben.
- **Explizite Musik und Podcasts zulassen** – Bei Markierung werden anstößige Musik oder Videoinhalt im iTunes Store angezeigt und nicht ausgeblendet. Anstößiger Inhalt wird bei der Aufführung im iTunes Store von den Inhaltsanbietern, wie z. B. Plattenfirmen, markiert.
- **Bewertung Region** – Wählt eine Bewertungsregion für Filme, TV-Sendungen und Anwendungen aus.
- **Filme** – Wählt die maximal zulässige Bewertung für Filme aus.
- **TV-Sendungen** – Wählt die maximal zulässige Bewertung für TV-Sendungen aus.
- **Anw.** – Wählt die maximale Anzahl von zulässigen Anwendungen aus.

Benutzerdefiniertes iOS-Konfigurationsprofil

Mobile > Profile > Profile erstellen >Neu/Bearbeiten > Benutzerdefiniertes iOS-Konfigurationsprofil

- Dieser Profiltyp wird auf iOS-Geräten unterstützt.
- Dieses Profil wird nicht auf Android- und Blackberry-Geräten unterstützt.

Das **benutzerdefinierte iOS-Konfigurations-Profil** ist ein Profil, das mithilfe des **iPhone-Konfigurationsprogramms** *(http://support.apple.com/kb/DL1466)* erstellt und in **Mobile Device Management** importiert wurde. Geben Sie die folgenden Angaben ein.

- **Name** – Der Name, mit dem das Profil in **Mobile Device Management** bezeichnet wird.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Konfigurationsdatei** – Führt eine Suche durch, um das zu importierende Konfigurationsprofil auszuwählen.

Geräteort und Tracking-Profil

Mobile > Profile > Geräteort und Tracking-Profil

- Dieser Profiltyp wird auf iOS-, Android- und Blackberry-Geräten unterstützt.

Geräteort und Tracking-Profil stellt Anmeldungs- und Standortoptionen auf Geräten ein. *Dies ist das einzige Profil, das für Blackberry-Geräte gilt.*

Tabellenspalten

- **Profiltyp** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **Check-in nur bei Verbindung mit WiFi** – Bei Markierung meldet sich der Agent nur an, wenn eine WiFi-Verbindung verfügbar ist. Diese Funktion wird noch nicht unterstützt.
- **Check-in nur bei Verbindung mit WiFi** – Bei Markierung meldet sich die Kaseya Agent-Anwendung nur an, wenn eine WiFi-Verbindung verfügbar ist. Ist diese Option nicht markiert, meldet sich die Kaseya-Anwendung per Mobilfunknetz an, wenn keine WiFi-Verbindung verfügbar ist.
- **Gerät nachverfolgen** – Bei Markierung ist Nachverfolgen aktiviert. Standortdaten werden anhand einiger vordefinierter Parameter gefiltert, um sicherzustellen, dass nur genaue und nützliche Standortdaten tatsächlich an VSA gesendet werden. *Aufgezeichnete Standortdaten werden erst an VSA gesendet, wenn der Agent sich zum nächsten Mal anmeldet.* Es werden folgende allgemeine Kriterien verwendet:
  - **Genauigkeit** – Jede Standortaktualisierung von einem GPS-Turm oder -Satelliten verfügt über eine Genauigkeitsbewertung, die einschätzt, wie sehr der Genauigkeit der Standortdaten aus der GPS-Quelle vertraut werden kann.
  - **Alter** – Ein Gerät speichert Standortdaten zwischen und überträgt manchmal alte Standortdaten an die **Kaseya Agent**-Anwendung, wenn seit längerer Zeit keine neue Standortaktualisierung abgerufen wurde.
  - **Zurückgelegte Distanz** – Die Strecke, die das Gerät seit der letzten Standortaktualisierung zurückgelegt hat. Diese kann null sein, wenn sich das Gerät nicht bewegt hat.
- **Anmeldezeit des Agent (Minuten)** –*Dieses Feld wird von installierten Agents ignoriert, die Version 1.1 oder höher der Kaseya Agent-Anwendung verwenden.* Stellt die Mindestdauer zwischen Anmeldeversuchen ein. Eine Anzahl von Umwelt- und Gerätebetriebsfaktoren bestimmt genau, wann die Anmeldung stattfindet. Je kleiner dieser Wert ist, umso mehr Akkustrom wird verbraucht.
- **Verfolgungspräzision (Meter)** – Dieser Wert wird an den GPS-Empfänger gesendet als Hinweis, wie genau die Durchgabe der Standortinformationen sein sollte. Je genauer die Anfrage ist, d. h. je kleiner der Wert, umso länger dauert der Standortabruf und umso mehr Strom wird verbraucht.
- **Mindestgenauigkeit vor Ignorieren (Meter)** – Dieser Wert regelt, welche Standortinformationen als nützlich genug angesehen werden, um an VSA gesendet und gespeichert zu werden. Wenn sich ein Gerät schnell bewegt – z. B. in einem Auto oder einem Zug – sind die Informationen der Standortnachverfolgung weniger genau und irgendwann nicht mehr nützlich. Standortpunkte, die weniger genau als dieser Wert sind, werden herausgefiltert und weder aufgezeichnet noch an VSA gesendet. Dieser Wert bestimmt mehr als alle anderen die Menge und Qualität der Standortinformationen, die vom Gerät gesendet werden.
- **Distanz für Verfolgungsbewegung** – Dieser Wert definiert die Mindestdistanz, die ein Gerät zurücklegen muss, in Metern, damit ein Standortaktualisierungsereignis ausgelöst und an den Agent gesendet wird. Es wird auch vom Agent verwendet, um zu entscheiden, ob der Standortpunkt aufgezeichnet und an VSA gesendet werden soll. Wenn dieser Wert zum Beispiel auf 500 Meter eingestellt ist und sich das Gerät nur 10 Meter bewegt, zeichnet der Agent diesen Punkt nur auf, wenn die **Min. / Max. Verfolgungszeit (Minuten)** dies zulässt.
- **Min. / Max. Verfolgungszeit (Minuten)** – Diese Werte definieren, wie oft Standortinformationspunkte aufgezeichnet werden sollen. Der Mindestwert definiert die Mindestzeit zwischen Punkten. Wenn

der Wert zum Beispiel 10 Minuten beträgt, dann werden die an den Agent gemeldeten Standortinformationen nach Meldung eines gültigen Standorts mindestens 10 Minuten lang nicht aufgezeichnet bzw. an VSA gesendet. Wenn jedoch innerhalb der vom maximalen Wert festgelegten Dauert kein gültiger Standortpunkt aufgezeichnet wurde, dann *wird* dieser Punkt aufgezeichnet, ohne Rücksicht auf Genauigkeit oder zurückgelegte Strecke.

Ein Beispiel für die Aufzeichnung eines Punkts:

- Ein Punkt wird bei angemessener Verfolgungsgenauigkeit abgefragt.
- Wenn der zurückgegebene Punkt einen höheren Genauigkeitswert als unter "Mindestgenauigkeit vor Ignorieren" angegeben hat, dann wird er verworfen.
- Wenn das Gerät nicht mindestens die unter "Distanz für Verfolgungsbewegung" angegebene Strecke zurückgelegt hat, wird der Punkt verworfen.
- Wenn die verstrichene Zeit zwischen diesem Punkt und dem letzten aufgezeichneten kürzer als die "Min. Verfolgungszeit" ist, wird der Punkt verworfen.
- Wenn die verstrichene Zeit zwischen diesem Punkt und dem letzten aufgezeichneten länger als die "Max. Verfolgungszeit" ist, dann wird der Punkt aufgezeichnet, auch wenn er durch die vorangehenden Prüfungen verworfen worden wäre.

WiFi-Profil

Mobile > Profile > WiFi-Profil

- Dieser Profiltyp wird auf iOS- und Android-Geräten unterstützt:
- Dieser Profiltyp wird nicht auf Blackberry-Geräten unterstützt.

Das **WiFi-Profil** stellt die WiFi-Optionen auf Geräten ein. Wegen der höheren Kosten, die bei der Datenübertragung per Mobilfunknetz entstehen, gibt es die Option, nur per WiFi mit VSA zu kommunizieren. Dies kann als Systemstandard angegeben werden oder durch Anwenden eines **Geräteort und Tracking-Profils** *(siehe 34)*. Wenn "Nur WiFi" aktiviert ist, kommunizieren Gerät und VSA nur dann, wenn das Gerät über eine WiFi-Verbindung verfügt. Sobald eine WiFi-Verbindung verfügbar ist, kann das Gerät eine Reihe von Befehlen verarbeiten, die in Warteschlange stehen, einschließlich Standortverfolgungsdaten. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.

Tabellenspalten

- **Profiltype** – Der Typ des Profils.
- **Name** – Der Name des Profils.
- **Beschreibung** – Eine Beschreibung des Profils.
- **SSID** – Ein eindeutiger Bezeichner eines drahtlosen Netzwerks.
- **Ausgeblendetes Netzwerk** – Bei Markierung sendet das drahtlose Netzwerk seine SSID nicht.
- **Verschlüsselungstyp** – Der Verschlüsselungstyp, der vom drahtlosen Netzwerk verwendet wird. Stellen Sie sicher, dass diese Werte genau mit den Eigenschaften des Netzwerkzugriffspunkts übereinstimmen. Wenn Sie unsicher bezüglich des Verschlüsselungstyps sind oder möchten, dass er für alle Verschlüsselungstypen gilt, verwenden Sie den Wert "Beliebig".
    - `WEP` - Wired Equivalent Privacy
    - `WPA` - WiFi Protected Access. Schließt sowohl WPA als auch WPA2 ein.
    - `Any` - Alle anderen Arten von WiFi-Protokollen
- **Kennwort** – Das WiFi-Kennwort.

Profile zuweisen

Mobile > Profile > Profile zuweisen

Die Seite **Profile zuweisen** weist Geräten Profile zu. Profile werden mit der Seite **Profile erstellen** *(siehe 28)* erstellt. Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Zuweisen von Profilen

1. Wählen Sie ein einzelnes Gerät aus dem mittleren Fensterbereich aus.
2. Klicken Sie auf die Schaltfläche **Zuweisen** im mittleren oder rechten Fensterbereich. Es wird eine Liste der verfügbaren Profile angezeigt.
3. Wählen Sie ein Profil aus der Liste aus.
4. Klicken Sie auf **Speichern**.

Entfernen von Profilen

1. Wählen Sie ein oder mehrere Geräte im mittleren Fensterbereich aus.
2. Wählen Sie ein Profil im rechten Fensterbereich aus.
3. Klicken Sie auf die Schaltfläche **Entfernen**.

Gerätetabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Besitzer** – Der Eigentümer des Geräts.

Profiltabellenspalten

- **Profiltyp**
  - **E-Mail-Profil** *(siehe 29)* – Konfiguriert den E-Mail-Client auf einem verwalteten mobilen Gerät. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.
  - **Sicherheitsprofil** *(siehe 30)* – Konfiguriert Richtlinien in Bezug auf die Erstellung von PINs. PINs werden von Gerätebenutzern verwendet, um ihre Geräte zu entsperren.
  - **Web Clip-Profil** *(siehe 31)* – Gibt eine Webanwendungsverknüpfung zu einer URL an, auf die das Gerät zugreifen kann. Gilt derzeit nur für iOS-Geräte. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden
  - **Geräte-Funktionsprofil iOS 4** *(siehe 31)* – Gilt für iOS-Geräte mit einer Version unter iOS 5. Aktiviert und deaktiviert beliebte Funktionen auf Geräten mit iOS 4.
  - **iOS-Geräte-Funktionsprofil** *(siehe 32)* – Gilt nur für iOS5, iOS6, iOS7. Aktiviert und deaktiviert beliebte Funktionen auf iOS-Geräten.
  - **Geräteort und Tracking-Profil** *(siehe 34)* – Stellt Anmeldungs- und Standortoptionen auf Geräten ein. Dies ist das einzige Profil, das für Blackberrys gilt.
  - **Benutzerdefiniertes iOS-Konfigurationsprofil** *(siehe 33)* – Ein Profil, das mithilfe des **iPhone-Konfigurationsprogramms** *(http://support.apple.com/kb/DL1466)* erstellt und in **Mobile Device Management** importiert wurde.
  - **WiFi-Profil** *(siehe 35)* – Stellt die WiFi-Optionen auf Geräten ein. Einem Gerät können mehrere Profile dieses Typs zugewiesen werden.
- **Name** – Name des Profils.
- **Details** – Ausgewählte Details zum Profil.

Gerätebenachrichtigungen

Mobile > Benachrichtigungen > Gerätebenachrichtigungen

Die Seite **Gerätebenachrichtigungen** stellt Alarmbedingungen für Geräte ein und kann optional eine Nachricht an ein oder mehrere Geräte senden. Zu den Benachrichtigungstypen gehören:

- **Gerät offline** – Das Gerät hat sich während der angegebenen Anzahl an Minuten nicht angemeldet.
- **Verlorenes Gerät checkt ein** – Ein Gerät meldet sich an, nachdem es als verloren gemeldet wurde.
- **Gerät checkt ein** – Ein Gerät meldet sich an.
- **Agent auffordern** – Fordert den Benutzer des Geräts auf, nachdem sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet hat. Gilt nur für iOS.
- **Nicht zugelassene Apps** – Auf einem Gerät wurde eine nicht zugelassene Anwendung ermittelt.
- **Erforderliche Apps** – Auf einem Gerät fehlt eine erforderliche Anwendung.

Die Liste der Geräte-IDs, die Sie auf dieser Seite auswählen können, hängt vom Geräte-ID-/Rechnergruppenfilter und dem verwendeten Scope ab.

Registerkarte "Übersicht"

Bietet eine Übersicht aller konfigurierten und für jedes Gerät aktivierten Alarmbedingungen.

Aktion

- **Nachricht senden** – Sendet eine Nachricht an ein oder mehrere ausgewählte Geräte. iOS-Geräte empfangen eine Push-Benachrichtigung. Android-Geräte empfangen eine SMS.

Tabellenspalten

- **(Gerätestatus)** – Der Status der Kaseya Agent-Anwendung auf dem Gerät des Benutzers.
  - Erstellt
  - Einladung fehlgeschlagen
  - Eingeladen – Es wurde eine Einladung an den Benutzer gesendet, um die Kaseya Agent-Anwendung auf dem Benutzergerät zu installieren.
  - Einladung abgelehnt
  - Installation läuft
  - Installation fehlgeschlagen
  - Normal – Die Anwendung ist installiert und funktioniert normal.
  - Befehl ausstehend
  - Befehl gesendet
  - Keine Antwort
  - Wird verarbeitet
  - Befehl gesendet – erneut versuchen
  - Abmelden
  - Befehl gesendet – fehlgeschlagen
- **(Geräte-BS)**
  - Android
  - Apple
  - Blackberry
- **Nachverfolgen** – Bei Markierung bzw. Anzeige des Nachverfolgungssymbols wird das Gerät nachverfolgt.
- **Gerätegruppen-ID** – Der Gerätebezeichner und die Rechnergruppe.
- **Besitzer** – Der Eigentümer des Geräts.
- **Telefonnummer** – Die Telefonnummer des Geräts. Einige mobile Geräte haben keine Telefonnummer.
- **Gerät offline** – Bei Markierung hat sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet.
- **Verlorenes Gerät checkt ein** – Bei Markierung hat sich ein Gerät angemeldet, das als verloren gemeldet ist.
- **Gerät checkt ein** – Bei Markierung meldet sich ein Gerät an.
- **Agent auffordern** – Bei Markierung wird der Benutzer des Geräts aufgefordert, nachdem sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet hat.

Registerkarte "Gerät offline"

Die Benachrichtigung **Gerät offline** tritt auf, wenn sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet hat.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Gerät offline**.
  - **Gerät hat nicht eingecheckt seit (Minuten)** – Gibt die Wartezeit in Minuten an, die seit der letzten Anmeldung des Geräts vergangen ist.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.

- **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger, die bei einer Alarmbedingung benachrichtigt werden.
- **Betreff** – Der Betreff der E-Mail-Nachricht.
- **Meldung** – Der Textkörper der E-Mail-Nachricht.

- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Registerkarte "Verlorenes Gerät checkt ein"

Die Benachrichtigung **Verlorenes Gerät checkt ein** tritt auf, wenn ein Gerät sich anmeldet, nachdem es als verloren gemeldet wurde.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Verlorenes Gerät checkt ein**.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger bei einer Alarmbedingung.
  - **Betreff** – Der Betreff der E-Mail-Nachricht.
  - **Meldung** – Der Textkörper der E-Mail-Nachricht.
- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Registerkarte "Gerät checkt ein"

Die Benachrichtigung **Gerät checkt ein** tritt auf, wenn ein Gerät sich anmeldet.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Gerät checkt ein**.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger bei einer Alarmbedingung.
  - **Betreff** – Der Betreff der E-Mail-Nachricht.
  - **Meldung** – Der Textkörper der E-Mail-Nachricht.

- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Registerkarte "Agent auffordern"

Die Benachrichtigung **Agent auffordern** fordert den Benutzer des Geräts auf, nachdem sich das Gerät während der angegebenen Anzahl an Minuten nicht angemeldet hat. Gilt nur für iOS-Geräte.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Agent auffordern**.
  - **Gerät hat nicht eingecheckt seit (Minuten)** – Gibt die Wartezeit in Minuten an, die seit der letzten Anmeldung des Geräts vergangen ist.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger bei einer Alarmbedingung.
  - **Betreff** – Der Betreff der E-Mail-Nachricht.
  - **Meldung** – Der Textkörper der E-Mail-Nachricht.
- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.
- **Nachricht jetzt senden** – Sendet die Aufforderung sofort.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Registerkarte "Nicht zugelassene Apps"

Die Benachrichtigung **Nicht zugelassene Apps** tritt auf, wenn auf einem Gerät eine nicht zugelassene Anwendung ermittelt wurde.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Nicht zugelassene Apps**.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger bei einer Alarmbedingung.
  - **Betreff** – Der Betreff der E-Mail-Nachricht.
  - **Meldung** – Der Textkörper der E-Mail-Nachricht.

- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Registerkarte "Erforderliche Apps"

Die Benachrichtigung **Erforderliche Apps** tritt auf, wenn auf einem Gerät eine erforderliche Anwendung fehlt.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Erforderliche Apps**.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger bei einer Alarmbedingung.
  - **Betreff** – Der Betreff der E-Mail-Nachricht.
  - **Meldung** – Der Textkörper der E-Mail-Nachricht.
- **Löschen** – Löscht die Alarmbedingung.
- **Aktivieren** – Aktiviert die Alarmbedingung neu.
- **Deaktivieren** – Deaktiviert die Alarmbedingung, ohne sie dauerhaft zu löschen. Während die Alarmbedingung deaktiviert ist, werden keine Benachrichtigungen erstellt.

> **Hinweis:** Diese Registerkarte enthält die gleichen Beschreibungen der Tabellenspalten wie oben angegeben.

Gruppenbenachrichtigungen

Mobile > Benachrichtigungen > Gruppenbenachrichtigungen

Die Seite **Gruppenbenachrichtigungen** erstellt eine Benachrichtigung, wenn ein neues Gerät einem ausgewählten Unternehmen oder einer Rechnergruppe beitritt. Die Liste der angezeigten Unternehmen und Rechnergruppen hängt von Ihrem **Scope** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4578.htm)* ab.

Aktion

- **Neu/Bearbeiten** – Erstellt oder bearbeitet die Alarmbedingung **Gruppenbenachrichtigungen**.
  - **Benachrichtigung über Wiederherstellung nach (Minuten)** – Nachdem die Benachrichtigung erstellt wurde, gibt dies die Zeit an, die vor dem Versenden einer weiteren E-Mail bzw. der Erstellung eines weiteren Tickets gewartet werden soll. Das Wiederherstellen wird abgebrochen, wenn die Alarmbedingung nicht mehr besteht.
  - **Ticket erstellen** – Erstellt ein Ticket als Reaktion auf die Alarmbedingung.
  - **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – E-Mail-Empfänger, die bei einer Alarmbedingung benachrichtigt werden.

   - **Betreff** – Der Betreff der E-Mail-Nachricht.
   - **Meldung** – Der Textkörper der E-Mail-Nachricht.
- **Löschen** – Löscht die Alarmbedingung.

Tabellenspalten

- **Name** – Der Name des Unternehmens oder der Rechnergruppe.

> **Hinweis:** Andere Tabellenspalten sind bereits oben definiert.

Systemeinstellungen

Mobile > System konfigurieren > Systemeinstellungen

Die Seite **Systemeinstellungen** stellt die Standardeinstellungen ein, die für alle von **Mobile Device Management** verwalteten Geräte gelten.

Systemeinstellungen

Beim Erstellen einer Einladung auf der Seite **Gerätestatus** *(siehe 10)* werden die folgenden Einladungsstandardwerte verwendet.

- **Server-ID** – Die eindeutige ID des Servers.
- **Standard-Landescode** – Der Standard-Landescode, der angezeigt wird, wenn sich das Dialogfenster für eine neue Einladung öffnet.
- **Standardgruppe** – Die Standardrechnergruppe, die angezeigt wird, wenn sich das Dialogfenster für eine neue Einladung öffnet.
- **Geräteeinladungsnachricht** – Der Text der Nachricht, der an den Benutzer gesendet wird, um ihn zur Installation eines mobilen Kaseya-Agent einzuladen. Wird verwendet, wenn der Administrator manuell ein neues Konto für ein bekanntes Gerät erstellt und eine Einladung zum Benutzer sendet, damit dieser den Agent installiert. Siehe **Installieren der Kaseya Agent-Anwendung** *(siehe 3)*.
- **App-Einladungsnachricht** – Der Text der Nachricht, der an den Benutzer gesendet wird, um ihn zur Installation einer erforderlichen Anwendung einzuladen. Siehe **Verwalten von Anwendungen auf Geräten** *(siehe 7)*.
- **Agentless Einladungsnachricht** – Der Text der Nachricht, der an den Benutzer gesendet wird, um ihn zur Installation eines mobilen Kaseya-Agent einzuladen.
- **Standardanzahl angezeigter Standortpunkte** – Begrenzt die Anzahl der anzuzeigenden Standortpunkte auf der Seite **Ein einziges Gerät nachverfolgen** *(siehe 23)*.

Nachrichten-Tags

Die folgenden Tags können in den auf dieser Seite angegebenen Einladungsnachrichten eingebettet werden.

- `{address}` = URL für Einladungsdienst
- `{serverId}` = Geräteserver-ID
- `{agentlessUrl}` = Bereitstellungs-URL
- `{name}` = Anwendungsname
- `{url}` = URL des Anwendungsspeicherorts

Webserver-Einstellungen

Die folgenden Felder überschreiben den Standard-Port 80 für HTTP- und Port 443 für HTTPS-Einstellungen und die Standard-URL `http://<your-KServer>/vsaWs/kmdmws.asmx`, die für den Zugriff auf **Mobile Device Management**-Webdienste verwendet wird.

- **Protokoll** – `HTTP` oder `HTTPS`
- **Externer Name / IP-Adresse des Servers**
- **Port für Webdienste**

Aktionen

- **Speichern** – Speichert die Änderungen an den Einstellungen dieser Seite.
- **Standardwerte verwenden** – Setzt diese Seite auf ihre ursprünglichen Werte zurück.

Server-Einstellungen

Mobile > System konfigurieren > Server-Einstellungen

Die Seite **Server-Einstellungen** stellt Serveroptionen für das **Mobile Device Management**-Modul ein.

Systemeinstellungen

- **Aufbewahrungszeit für Serverprotokolle** – Die Anzahl der Tage, während der Serverprotokolle gespeichert werden. Protokolle werden im `\<KServerInstallDirectory>\WebPages\ManagedFiles\Mobile\Logs`-Verzeichnis gespeichert.
- **Aufbewahrungszeit für App-Einladungsprotokolle** – Die Anzahl der Tage, während der App-Einladungsprotokolle gespeichert werden. Diese Protokolle werden in der Datenbank gespeichert.
- **Schwellwert für die Neuversendung von App-Einladungen** – Diese Anzahl der Tage wird gewartet, bis eine Einladung zur Installation einer erforderlichen Anwendung erneut an den Benutzer gesendet wird.

Aktionen

- **Speichern** – Speichert die Änderungen an den Einstellungen dieser Seite.
- **Standardwerte verwenden** – Setzt diese Seite auf ihre ursprünglichen Werte zurück.

Mobile Device Management Berichte

In diesem Abschnitt

Mobile Geräte – Geräteanwendungen

Info Center > Reporting > Berichte > Mobile Geräte - Geräteanwendungen

- *Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Geräteanwendungen** wird ein Bericht generiert, in dem die auf einem Gerät installierten Anwendungen aufgeführt sind.

Filter- und Sortierungsparameter

- **Betriebssystem-Typ** – `Android`, `Apple`
- **Hersteller** – Der Hersteller der Gerätehardware.
- **Original-Netzbetreiber** – Die Hauptnetzbetreiber für Geräte.
- **Aktueller Netzbetreiber** – Die Netzbetreiber, deren Services von Geräten derzeit verwendet werden.
- **Anwendungsname** – Der Name der auf Geräten installierten Anwendung.

Mobile Geräte – Gerätestatus

Info Center > Reporting > Berichte > Mobile Geräte - Gerätestatus

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsanwendung **Gerätestatus** wird ein Bericht generiert, in dem die Status eines jeden Geräts aufgeführt sind.

Filter- und Sortierungsparameter

- **Mobilgerätestatus** – *Nachstehend werden nur die gängigsten Befehle aufgeführt.*
  - `Eingeladen` – Dem Benutzer wird eine Einladung zugesandt, die Kaseya Agent-App auf dem Gerät des Benutzer zu installieren.
  - `Normal` – Die App ist installiert und funktioniert einwandfrei.
  - `Befehl ausstehend` – Aus dem Gerät des Benutzers steht ein Befehl für die Kaseya-Agent-App aus.
- **Betriebssystem-Typ** – `Android`, `Apple`
- **Verfolgen** – `True`, `False`

Mobile Geräte – Geräteübersicht

Info Center > Reporting > Berichte > Mobile Geräte - Geräteübersicht

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Geräteübersicht** wird ein Übersichtsbericht aller Auditinformationen von ausgewählten Rechnern generiert.

Filter- und Sortierungsparameter

- **Mobilgerätestatus** – *Nachstehend werden nur die gängigsten Befehle aufgeführt.*
  - `Eingeladen` – Dem Benutzer wird eine Einladung zugesandt, die Kaseya Agent-App auf dem Gerät des Benutzer zu installieren.
  - `Normal` – Die App ist installiert und funktioniert einwandfrei.
  - `Befehl ausstehend` – Aus dem Gerät des Benutzers steht ein Befehl für die Kaseya-Agent-App aus.
- **Betriebssystem-Typ** – `Android`, `Apple`
- **Hersteller** – Der Hersteller der Gerätehardware.
- **Original-Netzbetreiber** – Die Hauptnetzbetreiber für Geräte.

Anzuzeigende Detailtabellen

- **Detail zu Betriebssystem anzeigen**
- **Details für Geräteinfo anzeigen**
- **Plattformdetaildaten anzeigen**

- Details für Original-Netzwerk anzeigen
- Details für aktuelles Netzwerk anzeigen

Anzuzeigende Detailgrafiken

- Diagramm für Mobilgerätestatus anzeigen
- Diagramm für Betriebssystemart anzeigen
- Herstellerdiagramm anzeigen
- Diagramm für Original-Netzbetreiber anzeigen
- Diagramm für aktuellen Netzbetreiber anzeigen

Mobile Geräte – Verlorene Geräte

Info Center > Reporting > Berichte > Mobile Geräte – Verlorene Geräte

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Verlorene Geräte** wird ein Bericht aller verlorenen Geräte generiert.

Zeitrahmen

- **Von** – Filtert den Datumsbereich des Berichts nach diesem Startdatum.
- **Bis** – Filtert den Datumsbereich des Berichts nach diesem Enddatum.

Inhaltsverzeichnis

A

B

D

E

G

I

K

L

M

N

P

S

U

V

W